

MANOJ KUMAWAT

Senior Backend & Platform Engineer | Node.js · TypeScript · GraphQL · AWS · Cloudflare · AI Agents · Security

+91-9872509458 | hello@imkumawatmanoj.com | imkumawatmanoj.com | linkedin.com/in/imkumawat | github.com/imkumawat

SUMMARY

Senior Backend & Platform Engineer with 6 years of experience across product, AI, and security engineering, including 4+ years building e-commerce and subscription platforms serving 1.7M+ users, 400K+ active subscriptions, and 1.2M+ orders/year. Expertise in Node.js/TypeScript, GraphQL (Apollo), REST APIs, AI assistants, AI agent integration, and fault-tolerant event-driven architectures. Reduced AWS cloud spend by ~50% and built a monitored, idempotent payout pipeline processing \$150K+/month. Cybersecurity background (OWASP Top 10, VAPT) with experience designing secure systems through hardened authentication, scoped authorization, rate limiting, abuse prevention, and query complexity controls.

EXPERIENCE

Springworks

March 2022 – Present

Senior Backend Engineer — Burst Oral Care

Remote

- Designed and developed robust backend services powering an e-commerce platform serving 1.7M+ customers, 60K+ ambassadors on a mobile app, 400K+ subscriptions, and 1.2M+ orders/year, processing 500K+ API requests/day with high availability, low latency, and fault tolerance.
- Built REST and GraphQL APIs across admin dashboards, subscriptions, payments, and orders, holding p95 latency under production peak traffic via caching strategies, connection pooling, indexing, and query tuning.
- Designed and built an idempotent payout pipeline processing \$150K+/month in atomic Stripe transfers with automated reconciliation, engineered to prevent duplicate disbursements under retries and partial failures.
- Designed robust recurring subscription and order processing pipelines with automated retries, dead-letter queues, and exactly-once (idempotent) operations.
- Diagnosed and eliminated a query bottleneck that surfaced as the database grew — rewrote correlated subqueries into indexed JOINS with composite index design, cutting database CPU utilization and restoring stability under peak load.
- As sole DevOps owner, cut AWS spend ~50% (Aurora/RDS tuning, ECS/Kubernetes right-sizing, CloudWatch retention/log-ingestion tuning, Lambda concurrency tuning, S3 lifecycle policies) and hardened the edge with Cloudflare — WAF rules, rate limiting, and Turnstile bot protection on abuse-prone endpoints, plus Workers and Pages for edge logic and static delivery.
- Built internal admin tooling and self-service analytics dashboards for ops and business teams — replaced a \$2K/month hosted BI tool (Periscope/Sisense) with self-hosted Redash, eliminating ~\$24K/year in licensing.
- Built custom MCP (Model Context Protocol) servers and connectors for Claude in TypeScript, exposing internal systems (production database, AWS) as structured, read-scoped tools — enabling safe AI-assisted operations and investigation over production data without direct credential exposure.

Truminds Software Systems

July 2020 – February 2022

Security Engineer — Penetration Testing & VAPT

Gurgaon, India

- Performed end-to-end VAPT (vulnerability assessment & penetration testing) on web applications, REST APIs, and network infrastructure — combining manual exploitation on Kali Linux with Burp Suite, OWASP ZAP, sqlmap, Nessus, and Metasploit to uncover and exploit OWASP Top 10 flaws (SQL injection, broken access control, XSS, IDOR, auth bypass).
- Chained real-world attack paths — from injection and broken authentication to privilege escalation — and delivered detailed exploit walkthroughs, risk ratings (CVSS), and remediation guidance that engineering teams shipped to closure.
- Drove secure-by-design practices across teams — threat modeling, secure-coding reviews, and shift-left security in CI — eliminating recurring vulnerability classes and building the security instincts I now apply as a backend engineer.

PROJECTS

blue-node — backend reference implementation

2026

Node.js, TypeScript, Express 5, OAuth 2.1, MCP, Apollo GraphQL, Postgres, MongoDB, Redis, AWS github.com/imkumawat/blue-node

- Hand-rolled OAuth 2.1 authorization server — Dynamic Client Registration (RFC 7591), PKCE S256, server-rendered login and consent, discovery metadata (RFC 8414), resource-bound tokens (RFC 8707), and refresh-token rotation with reuse detection. Verified end-to-end against Claude Desktop as a real third-party client — from registration through consent to a tool call returning live data.

- MCP server (spec revision 2025-06-18) exposing the backend as scoped tools — per-tool scope enforcement, **aud** validation to prevent confused-deputy token reuse, and the **WWW-Authenticate** discovery chain that lets a client find the authorization server on its own. Written directly against the spec, without an SDK.
- Two token families, chosen by trust boundary — opaque, revocable first-party session tokens backing a per-device “where you’re logged in” list, and RS256 JWT access tokens for third parties signed with **jose**, carrying **kid** and verifiable from a published JWKS so keys rotate without downtime. No shared secrets anywhere.
- Modular monolith in TypeScript (ESM) on Express 5 — per-module REST + GraphQL (Apollo) adapters over Postgres (Drizzle), MongoDB, and Redis, plus an MQTT 5 broker client as a resilient shared transport (auto-reconnect, graceful degradation); BullMQ + standalone SQS worker for background jobs.
- Per-request DataLoader batching to eliminate resolver N+1 (order-preserving batch queries behind a request-scoped context), with query-complexity limits on incoming operations.
- Directive-driven GraphQL security at the schema level — **@authenticated**, **@requireScope**, **@rateLimit**, and alias-abuse protection — over a scoped permission system with per-IP and **per-(email|ip)** lockout, CAPTCHA step-up, and CSP-hardened server-rendered auth pages using escape-by-default templating, so the one value a third party chooses can never reach the page as markup.
- Multi-instance real-time layer — WebSocket transport with a connection manager and Redis Pub/Sub fan-out (rooms) so events reach clients across horizontally-scaled instances; graceful shutdown drains in-flight requests and jobs on SIGTERM, with pino logging and CI (GitHub Actions + Azure DevOps) running typecheck, lint, and Vitest gates.

SKILLS

- **Languages:** TypeScript, JavaScript (Node.js, ES6+), Python
- **Database:** MySQL (Aurora), PostgreSQL, MongoDB, Redis, ClickHouse
- **Backend & API:** GraphQL (Apollo — Federation, Subscriptions), REST, Express 5, Hono, Zod, OAuth 2.1 authorization server (DCR, PKCE, JWKS, resource indicators), OIDC, JWT (jose, RS256), MCP, ORMs (Drizzle, Sequelize, Mongoose), connection pooling, Webhooks, WebSockets, Server-Sent Events (SSE), DataLoader, API versioning, idempotency keys, cursor-based pagination, OpenAPI/Swagger
- **Integrations:** Stripe, Shopify, Recharge, Klaviyo, TaxJar/Numeral, ShipHero, SendGrid, Twilio
- **Frontend:** Next.js, React, Tailwind CSS
- **AI & LLM Tooling:** Anthropic Claude API, OpenAI API, Prompt Engineering, LLM Integration, Function Calling / Tool Calling, RAG & Vector DB, MCP & Connectors for Claude, AI Assistants, AI Agents, Agentic AI, AI-assisted development (Claude Code)
- **Messaging & Events:** Apache Kafka, AWS SQS/SNS/EventBridge/Kinesis, BullMQ, MQTT 5, event-driven architecture
- **Cloud & DevOps:** AWS (ECS/Fargate, EKS, ECR, EC2, Lightsail, Lambda, API Gateway, Aurora/RDS, DynamoDB, ElastiCache, Redshift, Airflow, S3/Glacier, CloudFront, Route53, WAF, IAM & Identity Center, Cognito, Secrets Manager), Cloudflare (Workers, Pages, Containers, Durable Objects, Queues, Workflows, R2, KV, D1, WAF, Rate Limiting, Turnstile, Zero Trust, DNS, Load Balancing), Azure (Functions, Container Apps, Blob Storage, Front Door), Kubernetes, Docker, CI/CD (GitHub Actions, Azure Pipelines, CodePipeline, CodeBuild), Systemd, Nginx
- **Security:** OWASP Top 10, VAPT (Kali Linux, Burp Suite, OWASP ZAP, Nessus, sqlmap, Metasploit), SAST (SonarCloud), secure coding, refresh-token reuse detection, rate limiting, JWKS key rotation, scoped delegation, CSP, escape-by-default templating
- **Observability:** CloudWatch, OpenSearch, Sentry, structured logging (pino)
- **Architecture:** Modular monolith, Domain-Driven Design (DDD), Clean / Hexagonal architecture, Backend-for-Frontend (BFF)
- **Practices & Delivery:** Agile development (Scrum), Jira, Azure DevOps

EDUCATION

Lovely Professional University
B.Tech in Computer Science & Engineering

Punjab, India
July 2016 – June 2020