



<https://efficienza.in/job/python-backend-engineer-2-4-yrs/>

Python Backend Engineer (2–4 Yrs)

Description

Role Overview

Efficienza is looking for a mid-senior Python Backend Engineer to design and build secure, scalable backend services for enterprise applications. The core of this role is authentication, authorization, and identity management, alongside building reliable API integrations with communication and notification providers.

You will own backend features end to end: designing APIs, implementing identity and access flows with Keycloak and Amazon Cognito, integrating messaging services such as Twilio, SendPulse, and SMTP, and building the data and caching layers on PostgreSQL and Redis. You will work closely with frontend engineers, DevOps, and product to ship features that are secure by design and stable in production.

This role suits an engineer who has moved past writing isolated scripts and now thinks about service boundaries, security, and integration reliability as first-order concerns.

You will excel if you:

Write backend code with security, observability, and maintainability in mind from the first commit

Design API contracts that are predictable, well-documented, and safe for other teams to depend on

Handle third-party integrations defensively, anticipating timeouts, retries, and failure states

Treat authentication and authorization as core architecture, not a feature

Take ownership of features end to end and follow through on production issues

Key Responsibilities

Backend Services and API Development

Design, build, and maintain RESTful backend services using FastAPI and Flask following consistent conventions

Define clear API contracts with request validation, structured error handling, and predictable response formats

Build reusable backend modules and utilities that reduce duplication across services

Write maintainable, testable code with unit and integration coverage using pytest

Optimise backend performance: query efficiency, caching strategy, and response latency under load

Authentication, Authorization and Identity

Implement and maintain authentication flows using Keycloak

Integrate Amazon Cognito for user pools, identity federation, and token-based authentication where required

Design and enforce authorization models: role-based and attribute-based access

Hiring organization

Efficienza Business Solutions

Employment Type

Full-time

Job Location

Chennai

Experience

2-4 Years

Date posted

July 16, 2026

control across services

Manage JWT issuance, validation, refresh, and revocation securely across the backend

Implement secure session handling, token storage strategy, and protection against common auth vulnerabilities

Document identity and access flows clearly so frontend and other services can integrate them correctly

Data, Caching and Storage

Design and maintain PostgreSQL schemas with appropriate normalisation, indexing, and constraint design

Write and optimise queries using SQLAlchemy ORM and raw SQL where performance demands it

Manage database migrations cleanly using Alembic without breaking existing data or dependent services

Use Redis for caching, session storage, rate limiting, and ephemeral state with appropriate expiry strategies

Ensure data consistency across the request lifecycle and validate frontend-to-backend data integrity

Reliability, Security and Operations

Implement structured logging, exception handling, and monitoring across all backend services

Apply security best practices: input validation, secrets management, least-privilege access, and dependency hygiene

Troubleshoot production issues with urgency and provide root-cause resolutions, not just patches

Collaborate with DevOps on CI/CD pipeline integration and deployment automation

Ensure coding standards, security guidelines, and review practices are consistently followed

Collaboration and Technical Leadership

Participate in code reviews, technical discussions, and architecture planning with a focus on long-term maintainability

Work with stakeholders to translate requirements into clear technical designs and API specifications

Provide technical guidance to junior engineers on backend patterns, security, and integration design

Contribute to backend documentation: service guides, API references, and integration runbooks

Area	Proficiency	Details
Python	Core Strength	Backend development, OOP, async patterns, clean modular code
FastAPI / Flask	Core Strength	REST API design, validation, middleware, dependency injection
Auth & Identity	Core Strength	Keycloak, JWT lifecycle, RBAC and ABAC, secure session handling
Amazon Cognito	Proficient	User pools, identity federation, token-based authentication
Twilio	Proficient	SMS, voice, notifications, webhook handling, delivery tracking
SendPulse / SMTP	Proficient	Transactional and bulk email, delivery status, provider integration
PostgreSQL	Proficient	Schema design, query optimisation, indexing, constraints
SQLAlchemy / Alembic	Proficient	ORM modelling, raw SQL, migration management
Redis	Proficient	Caching, session storage, rate limiting, expiry strategies
Git & CI/CD	Experienced	Branching, pull requests, pipeline integration, deployment flow
pytest	Proficient	Unit and integration testing, fixtures, mocking external services

Good to Have

Experience with AWS services beyond Cognito: S3, Lambda, SQS, Secrets Manager, or CloudWatch
Familiarity with Docker and containerised local development and deployment
Exposure to async task processing with Celery, RQ, or similar job queue systems
Understanding of OAuth 2.0 and OpenID Connect flows beyond basic token handling
Experience with message queues such as RabbitMQ or Kafka for event-driven architecture
Awareness of API gateway patterns and service-to-service authentication
Exposure to LLM API integration and AI-assisted backend automation workflows

Key Deliverables

Secure, well-documented backend APIs built to agreed standards with test coverage
Reliable authentication and authorization flows across Keycloak and Cognito, fully

documented for integration

Resilient messaging integrations with Twilio, SendPulse, and SMTP that handle failure states gracefully

Clean database schemas, migrations, and caching layers that scale with product growth

Production-stable services with logging, monitoring, and clear runbooks for on-call resolution

What Success Looks Like

Authentication and authorization flows are secure, well-documented, and rarely the source of production incidents

Third-party integrations fail gracefully and recover automatically, rather than cascading into outages

Other engineers can integrate your APIs from documentation alone, without needing to ask how they work

Production issues in your areas are resolved at the root cause and do not recur in the same form

Your backend work raises the security and reliability bar for the team rather than adding to its maintenance load

Educational Qualification

Bachelor's degree in Computer Science, Information Technology, Engineering, or a related field