Backend & API Layer (Core System)

Purpose: Public REST API, session handling, auth, callback

- **Language:** Python 3.10+
- **Framework:** FastAPI
    - Async, fast, clean OpenAPI docs
- **Auth:** API Key (x-api-key)
- **Validation:** Pydantic
- **Server:** Uvicorn / Gunicorn
- **Deployment:** Docker + Cloud VM / Container

FastAPI maps **perfectly** to the required request/response JSON structure and is easy to debug during evaluation.

Scam Detection Engine (Intent Classifier)

Purpose: Decide *when* to activate the agent

Option A (Best for Hackathon):

- Keyword + pattern rules (UPI, urgency, threats)
- Regex + scoring
- Lightweight ML (TF-IDF + Logistic Regression)

Option B (Advanced):

- Fine-tuned transformer (DistilBERT / IndicBERT)

Hybrid approach = **high accuracy** + **fast response time**

Agentic AI Conversation Engine

Purpose: Human-like multi-turn engagement

- **LLM:** OpenAI GPT-4 / GPT-4.1 / GPT-4o-mini
- **Agent Framework:** LangGraph or LangChain
- **Memory:** Conversation buffer (session-scoped)

- **Persona Prompt:**
    - Curious
    - Slightly confused
    - Never confrontational
    - Never reveals detection

Key scoring area: **believability + depth**

Intelligence Extraction Module

Purpose: Structured intelligence for final callback

- Regex + NLP extraction for:
    - UPI IDs
    - Bank account numbers
    - Phone numbers
    - URLs
    - Scam keywords
- Post-processing:
    - Deduplication
    - Confidence tagging

Output exactly matches:

```
extractedIntelligence {
  bankAccounts
  upiIds
  phishingLinks
  phoneNumbers
  suspiciousKeywords
}
```

Session & State Management

Purpose: Multi-turn continuity

- Redis (preferred) or in-memory store
- Session-keyed:

    - Message count
    - Scam confidence
    - Agent status
    - Intelligence buffer

Final Callback & Reporting

Purpose: Mandatory GUVI evaluation submission

- HTTP client: requests / httpx
- Retry + timeout logic
- Callback only when:
    - scamDetected = true
    - Engagement complete

Missing this = disqualification

Infra, DevOps & Monitoring

- Docker (mandatory)
- Logging: Loguru / Python logging
- Error tracking (basic)
- Cloud: Amazon Web Services / GCP / Azure
- CI (optional): GitHub Actions

System Architecture (Mental Model)

Incoming Message

↓

Scam Detection Engine

↓ (if scam)

Agent Controller

↓

LLM Agent (multi-turn)

↓

Intelligence Extractor

↓

Final Callback to GUVI