JIRA Ticket – AskBot

Internal GenAI Assistant for Enterprise Services

Project: Internal GenAI Platform – AskBot

Summary: Build a secure, role-aware, GenAI-powered internal assistant to handle HR, Payroll, Training, and Insurance queries via LLMs, scoped agents, and secure system APIs.

Owner: Security Architecture / LLM Applications Product Team

Created: June 2025

Maturity Level: MCP-Aware, Agentic-Controlled Execution, RBAC-Scoped Plugins

Objective

AskBot is a secure, GenAI-enabled enterprise assistant embedded into the employee portal. It empowers employees to self-serve through natural language interactions while enforcing security, observability, and permission boundaries using agentic control and task-scoped tool execution (MCP model).

Key Functional Modules

- LLM Orchestration
- Agent Router
- Scoped Plugins (Tools)
- Context Memory & Observability
- Guardrails + Redaction Layer
- Vault Integration
- RBAC Enforcement (MCP style)

Integrated Agents, Tools, and APIs

Includes API path, new vs. existing, purpose, and data handled. See table in workshop handout for full matrix.

Agent / Tool	API Invoked	New or Existing	Purpose / Functionality	Data Handled
Payslip Agent	/api/payroll/payslip/{month}	✅ Existing	Fetch PDF copy of payslip	Name, Salary, PAN, Bank Account
Salary Breakdown Tool	/api/payroll/breakdown	✅ Existing	Return earnings/deductions	Component-wise salary details
HR Policy Agent	/api/hr/policies/search	✅ Existing	Answer HR policy queries	Text-based responses, policy categories
Leave Balance Agent	/api/hr/leave/balance	✅ Existing	Show current leave balance	UserID, Leave counts
Training Agent	/api/training/courses/assigned	✅ Existing	List current trainings	UserID, CourseIDs
Insurance Agent	/api/insurance/summary	✅ Existing	Show insurance coverage	UserID, InsuranceID, Tiers
Claim Status Checker	/api/insurance/claim/{claimId}	✅ Existing	Track status of medical claims	ClaimID, PII, Medical Records
Routing Agent	/api/escalation/create	🆕 New	Raise unresolved issue to HR/Admin	UserID, Query Metadata
Agent Router (MCP)	internal/task_router/dispatch	🆕 New	Validates scope, dispatches tools	Agent Name, Role, Intent
PII Redaction Layer	Intercepts before LLM output	✅ Existing (lib)	Regex, ReLLM, LangChain filtering	Name, PAN, Email, Bank
Secrets Vault	vault/api/token/read	✅ Existing	Fetch API tokens securely	Plugin Tokens, Role Credentials

Security Architecture & Controls

- Prompt Injection: Guardrails + Regex Validation + Schema Enforcement
- Agent Misuse (MCP): Scoped tool access via Agent Router
- Sensitive Data Leakage: Real-time PII masking
- Over-Privilege: RBAC-scoped plugins only
- Token Exposure: Vault-only runtime access
- LLM Overreliance: Escalation to HR if confidence drops

Data Categories Handled

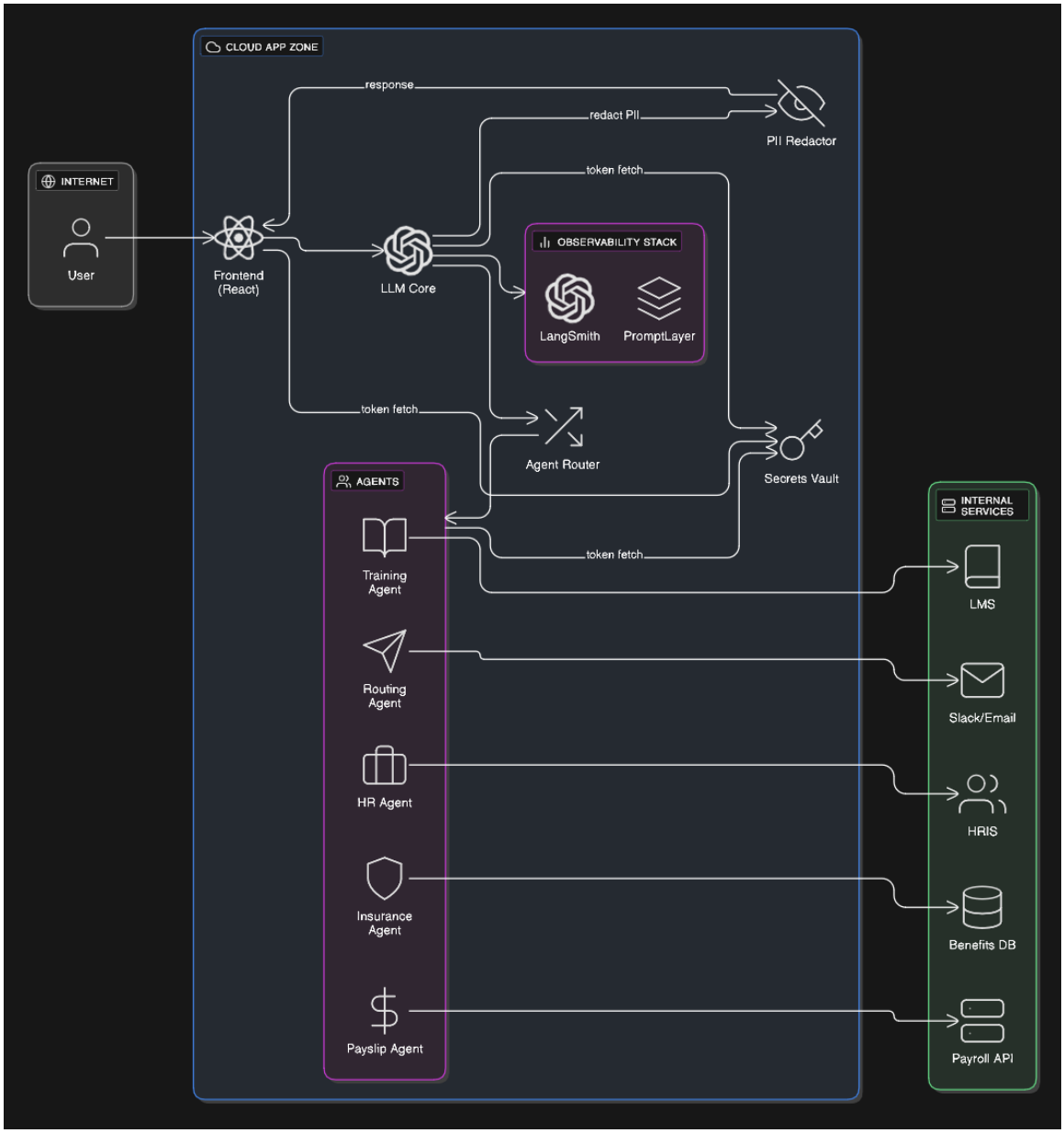
- PII: Name, Email, PAN, EmployeeID
- Salary & Compensation: HRA, Tax Components
- Health/Insurance: Claim ID, TPA Data
- Training: Assigned course metadata
- HR Policies: Internal knowledge base access

System Architecture Summary

1. User input → LLM
2. LLM → Agent Router
3. Agent → Internal API via Vault token
4. Output → Guardrails + Redaction
5. Response → Web UI

Acceptance Criteria

- Agent logs must include prompt history and trace ID
- Vault secrets are never cached or exposed
- Guardrails validated against test cases
- Escalation must work when confidence drops
- All plugin access must validate via MCP Router
- Threat Modeling artifact must be attached


CLOUD APP ZONE
response
redact PII
PII Redactor
token fetch
INTERNET
User
Frontend (React)
LLM Core
OBSERVABILITY STACK
LangSmith
PromptLayer
token fetch
Agent Router
Secrets Vault
AGENTS
INTERNAL SERVICES
token fetch
Training Agent
LMS
Routing Agent
Slack/Email
HR Agent
HRIS
Insurance Agent
Benefits DB
Payslip Agent
Payroll API

☑ Functional Use Cases (Agile Format)

Payslip Download

- As an employee, I want to ask AskBot for my last 3 months' payslips so that I can download and review them easily.

Leave Balance Check

- As an employee, I want to know how many casual leaves I have left so I can plan my time off effectively.

Training Completion Status

- As an employee, I want to ask AskBot if I have any pending compliance trainings so I can stay compliant.

Insurance Claim Status

- As an employee, I want to know the status of my latest insurance claim so I can follow up with HR if needed.

Policy Reference

- As a new hire, I want to ask about the company’s travel reimbursement policy so I don’t miss eligible claims.