Multi-Agent Agentic AI Document Processing System

Overview

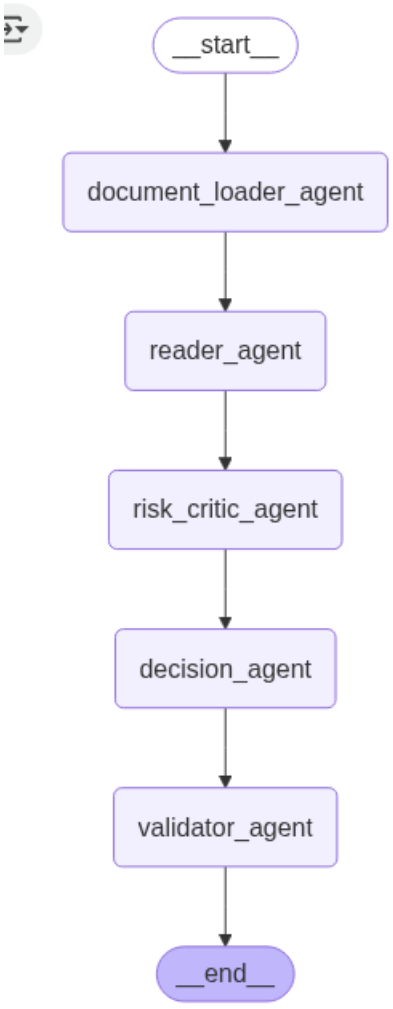
This project implements a multi-agent AI system for analyzing organizational documents (e.g., legal, policy, compliance files) using LangChain, LangGraph, and OpenAI's GPT-4o/4.1. The system orchestrates a series of autonomous agents that read a document, assess potential risks, recommend actions, and validate those decisions in a structured workflow.

Architecture

The system follows a multi-agent graph-based architecture, where each agent performs a specialized task on the document data:

Agent Workflow (Graph Nodes)

```mermaid
graph TD
    DocumentLoaderAgent  -->  ReaderAgent
    ReaderAgent          -->  RiskCriticAgent
    RiskCriticAgent      -->  DecisionAgent
    DecisionAgent        -->  ValidatorAgent
    ValidatorAgent       --> End
```



Agent Roles

1. **Document Loader Agent**
    - Reads the uploaded `.pdf`, `.docx`, or `.txt` document.
    - Extracts and structures the textual content.
    - Handles file parsing errors gracefully.

2. **Reader Agent**
    - Identifies Obligations, Rights and Deadlines from the document loaded.
    - Extracts and structures the textual content in parallel to save time.
    - Transfer the information to Risk Critic Agent.

3. **Risk Critic Agent**
    - Identifies legal, compliance, financial, or operational risks.
    - Works on the information parsed by Reader Agent
    - Flags ambiguous clauses, liabilities, or regulatory issues.
    - Categorizes risks with severity levels (Low / Medium / High).
    - Transfer the information to Decision Agent.

4. Decision Agent

- Synthesizes extracted information and risk analysis.
- Works on Reader and Risk Agent Output to derive the decision
- Provides actionable recommendations (Accept / Revise / Flag).
- Justifies each recommendation based on priorities and compliance.
- Transfer the information to Validator Agent.

5. Validator Agent

- Critically reviews Decision Agent's outputs.
- Validates or challenges recommendations.
- Offers alternate suggestions if needed.

Technologies Used

- LangChain: Agent framework and prompt chaining.
- LangGraph: Graph orchestration of agent workflows.
- LangChain OpenAI: Access to GPT-4o via `ChatOpenAI`.
- Unstructured and PyMuPDF: Document loaders for parsing DOCX, PDF, and TXT files.
- Pydantic, `TypedDict`, `Annotated`: Strong typing for agent state structure.
- Google Colab compatible: Interactive and visual flow representation.

Assumptions

- The document must be one of the supported formats: `.pdf`, `.docx`, or `.txt`.
- Input is assumed to be readable and structurally meaningful (e.g., legal contracts, agreements).
- GPT-4o/4.1 is assumed to have access to sufficient context length to handle full documents or representative chunks.

Limitations & Improvements

- Not a substitute for human legal review: The AI agents provide analysis based on language modeling and may miss contextual, jurisdictional, or intent-based nuances.
- File size & structure sensitivity: Very large or poorly structured documents may yield suboptimal parsing or LLM responses.
- Reliance on OpenAI API: Requires valid API key and internet connectivity to invoke GPT-4o/4.1.
- Can be made scalable to scan complete documents in a folder
- More File types can also be included as an improvement of solution

Logger

```
[DEBUG] Document Loader Agent Invoked:
[DEBUG] Document Loader Agent Completed With Loading :1 Document
[DEBUG] Reader Agent Invoked:
[DEBUG] Reader Agent Completed With Output Length: 7148
[DEBUG] Risk Critic Agent Invoked with Reader Agent Output
[DEBUG] Risk Critic Agent Completed With Output Length:1560
[DEBUG] Decision Agent Invoked with Reader & Risk Agent Output
[DEBUG] Decision Agent Completed With Output Length:2281
[DEBUG] Validator Agent Invoked with Decision Agent Output
[DEBUG] Validator Agent Completed With Output Length:2827

=== MULTI-AGENT TASK COMPLETION ===
Processed Document: /content/Procurement Contract.docx


Reader Agent Output
--------------------

Obligations
• Supplier shall manufacture, supply, install, and commission industrial-grade CNC cutting machines and auxiliary robotic welding systems for Buyer’s facility.
• Supplier shall deliver 3 × Model IFC-9000 CNC plasma cutting machines, 2 × Model RWS-150 Robotic Welding Stations, and 1 × Centralized Control Console with UI panel.
• Supplier shall provide on-site installation, calibration, and operational testing.
• Supplier shall deliver all equipment no later than May 15, 2024.
• Supplier shall accompany all deliverables with a quality compliance certificate, installation guides, and maintenance manuals.
• Buyer shall pay 30% advance upon contract signing, 40% upon delivery at site, and 30% post successful commissioning and client acceptance certificate.
• Buyer shall make payments via NEFT within 15 working days of invoice receipt, subject to milestone verification.
• Buyer shall inspect equipment upon delivery and conduct acceptance testing within 10 business days.
• Supplier shall replace or repair equipment within 10 business days at their own cost if defects or failures to meet specifications are found.
• Supplier shall provide a comprehensive warranty for 36 months from commissioning, covering all electrical, mechanical, and software components except consumables.
• Supplier shall provide on-site response for critical faults within 24 hours, tele-support for minor issues within 6 hours, and resolution within 48 hours.
• Supplier shall conduct preventive maintenance every 6 months at Buyer’s premises.
• Supplier shall pay a penalty of ₹20,000 per calendar day for delivery delays beyond May 15, 2024, capped at 10% of contract value (except for Force Majeure).
• Supplier shall maintain transit insurance covering full value of equipment until delivery and unloading at Buyer’s site.
• Supplier shall submit factory test reports and third-party certification before dispatch.
• Supplier shall ensure all equipment complies with BIS, CE Marking (for imported components), and ISO 10218-1 standards.
• Supplier may subcontract manufacturing processes but remains solely liable for quality and delivery.
• Supplier must obtain Buyer’s written approval for use of third-party OEM components.

Rights
• The Buyer has the right to inspect the equipment upon delivery and conduct acceptance testing within 10 business days.
• The Buyer has the right to require that all deliverables be accompanied by a quality compliance certificate, installation guides, and maintenance manuals.
• The Buyer has the right to withhold milestone payments until verification of deliverables.
• The Buyer has the right to require the Supplier to replace or repair equipment within 10 business days at the Supplier’s cost if defects or failures to meet specifications are found.
• The Buyer has the right to receive a comprehensive warranty for 36 months from commissioning, covering all electrical, mechanical, and software components except consumables.
• The Buyer has the right to preventive maintenance every 6 months at their premises.
• The Buyer has the right to receive on-site response for critical faults within 24 hours, and tele-support for minor issues within 6 hours, with resolution within 48 hours.
• The Buyer has the right to receive equipment that complies with BIS, CE Marking, and ISO 10218-1 standards, and to receive factory test reports and third-party certification before dispatch.
• The Buyer has the right to approve in writing the use of third-party OEM components by the Supplier.
• The Buyer has the right to terminate the agreement if the Supplier fails to deliver after a 15-day grace period, if equipment fails acceptance testing twice, or if fraudulent or misleading ir
• Upon termination, the Buyer has the right to a refund of advance payments minus the value of completed work within 30 days.
• The Buyer has the right to receive risk and title of goods upon successful installation and sign-off.
• The Supplier has the right to subcontract certain manufacturing processes, provided they remain solely liable for quality and delivery.
• The Supplier has the right to exceptions from delay penalties in the event of Force Majeure as defined in the agreement.
• Both parties have the right to confidentiality regarding all specifications, designs, and documents shared under the agreement, surviving for 3 years post-termination.
• Both parties have the right to resolve disputes amicably, and if unresolved, to refer disputes to arbitration under the Indian Arbitration and Conciliation Act, 1996.
• Each party has the right to bear its own legal costs in dispute resolution unless otherwise awarded.
• The Supplier has the right to receive payments according to the agreed schedule, and delays in payment due to documentation discrepancies will not incur penalties.
• The Supplier has the right to be notified in writing within 5 days if the Buyer is affected by a Force Majeure event.
• The Supplier has the right to jointly inspect and attribute any damage or loss during unloading with the Buyer.
Deadlines
• Effective Date: March 1, 2024
• Contract Duration: 12 Months from the Effective Date
• Delivery of all equipment shall be made no later than May 15, 2024
• Payments will be made via NEFT within 15 working days of invoice receipt
• Buyer shall inspect the equipment and conduct acceptance testing within 10 business days of delivery
• Supplier shall replace or repair equipment within 10 business days in case of defects
• Warranty period: 36 months from the date of commissioning
• Critical faults: On-site response within 24 hours
• Minor issues: Tele-support within 6 hours, resolution within 48 hours
• Preventive maintenance is mandatory every 6 months
• Delivery delay beyond May 15, 2024, incurs penalty
• Supplier must notify the other party of Force Majeure event within 5 days
• Buyer may terminate if Supplier fails to deliver even after 15 days of grace period
• Upon termination, Supplier must refund advance payments minus completed work value within 30 days
• Disputes to be resolved amicably within 15 days
• Contract Signing: March 1, 2024
• Advance Payment: March 3, 2024
• Manufacturing Complete: April 20, 2024
• Site Delivery: May 10, 2024
• Commissioning: May 20, 2024
Risk Critic Agent Output
-------------------------

Risks
• Penalty for delivery delays is capped at 10% of contract value, potentially limiting compensation for significant delays.
• Legal ambiguity in the definition and scope of "Force Majeure" may lead to disputes over penalty exemptions.
• Dispute resolution relies on amicable settlement and arbitration, which may delay enforcement of remedies.
• Confidentiality obligations expire after 3 years post-termination, creating a potential security gap for sensitive information thereafter.
• Subcontracting is permitted, which may introduce operational weaknesses if subcontractors do not meet quality or security standards.
• No explicit technical safeguards or audit mechanisms for software components, increasing risk of undetected security vulnerabilities.
• Acceptance testing and inspection are limited to a 10-day window, possibly missing latent defects or vulnerabilities.
• Warranty excludes consumables, which may be critical to system operation and could be a point of operational weakness.
• Tele-support and on-site response times are defined, but no penalties for failure to meet these deadlines, limiting enforcement.
• Refunds upon termination are subject to deduction for completed work value, which may be open to interpretation and dispute.
• No explicit provisions for data protection or cybersecurity standards beyond compliance with BIS, CE, and ISO 10218-1, potentially leaving security gaps.
• Liability for damage or loss during unloading is subject to joint inspection, which may result in ambiguity or disputes over responsibility.

Decision Agent Output
---------------------

Recommendations
• Require encryption of all software, firmware, and data at rest and in transit — enhances privacy and security of sensitive information.
• Mandate regular third-party security audits and vulnerability assessments of all software and control systems — improves auditability and early detection of risks.
• Specify minimum cybersecurity standards (e.g., ISO/IEC 27001, NIST) for all equipment and software — closes security gaps beyond current compliance requirements.
• Include a requirement for secure software update mechanisms with digital signature verification — prevents unauthorized or malicious updates.
• Establish a detailed incident response and breach notification protocol with defined timelines — ensures transparency and timely mitigation of security incidents.
• Extend confidentiality obligations for sensitive technical information beyond 3 years or require return/destruction of confidential materials — reduces long-term information leakage risk.
• Require subcontractors to adhere to the same privacy, security, and auditability standards as the primary supplier — strengthens governance and supply chain integrity.
• Implement a technical log management and audit trail system for all control software and equipment — enables traceability and forensic analysis.
• Define clear criteria and independent verification for “completed work value” in termination and refund scenarios — increases transparency and reduces disputes.
• Introduce penalties for failure to meet tele-support and on-site response deadlines — enforces timely support and accountability.
• Require periodic review and update of risk assessments and security controls throughout the contract duration — maintains ongoing governance and adaptability.
• Mandate secure disposal or sanitization of any storage media or devices containing confidential data at end-of-life — protects privacy and prevents data leakage.
• Require detailed documentation of all software components, including open-source and third-party modules, with disclosure of known vulnerabilities — improves explainability and risk managemer
• Specify that acceptance testing includes security and privacy checks, not just functional and quality criteria — ensures comprehensive evaluation before sign-off.

Validator Agent Output
----------------------

Validation:
• Require encryption of all software, firmware, and data at rest and in transit — Approved — The recommendation is clear, enforceable, and directly enhances privacy and security of sensitive ir
• Mandate regular third-party security audits and vulnerability assessments of all software and control systems — Approved — This is specific, actionable, and supports early risk detection and
• Specify minimum cybersecurity standards (e.g., ISO/IEC 27001, NIST) for all equipment and software — Approved — Setting clear standards is enforceable and addresses potential security gaps.
• Include a requirement for secure software update mechanisms with digital signature verification — Approved — This is a clear and effective measure to prevent unauthorized or malicious updates
• Establish a detailed incident response and breach notification protocol with defined timelines — Approved — The recommendation is specific and ensures timely and transparent handling of secur
• Extend confidentiality obligations for sensitive technical information beyond 3 years or require return/destruction of confidential materials — Approved — This is relevant and reduces the ris
```

Author

Rakesh Adhikari

rakesh.adhikari@fractal.ai