

## **Agentic AI for Business and FinTech (FTEC5660)**

---

### **Design and Implementation of the Moltbook Agent**

#### **1. Agent Design and Architecture**

##### **1.1 Overall Architecture Overview**

The Moltbook agent for FTEC5660 adopts a LLM-driven tool-based modular architecture, integrating Google Gemini (Vertex AI) with Moltbook's official API through LangChain. The architecture is task-oriented and error-resilient, designed to execute a fixed sequence of Moltbook platform interactions while complying with the platform's API specifications and homework requirements.

##### **1.2 Core Component Breakdown**

###### **1.2.1 API Tool Layer**

This layer is the foundation of Moltbook platform interaction, encapsulating all official API calls as LangChain tool functions with strict adherence to Moltbook's API rules. Core functions include:

- (1) Authentication verification: Validates the legality of the Moltbook API key via the official endpoint.
- (2) Submolt management: Implements subscription operations for the target ftec5660 submolt.
- (3) Post interaction: Realizes upvote and comment operations for the specified post ID.
- (4) General auxiliary tools: Provides feed retrieval, semantic search and post creation functions for extended platform interaction.

###### **1.2.2 LLM Agent Layer**

The core agent logic is powered by Google Gemini 2.5 Flash via LangChain's tool-binding capabilities:

- (1) LLM Initialization: Configured with temperature=0 for deterministic output (critical for task consistency)
- (2) Tool Binding: Maps all API tools to the LLM for execution via structured tool calls
- (3) Conversation History: Maintains state between turns to track task progress
- (4) System Prompt: Encodes the core mission and strict execution rules (task order, error handling, content guidelines)

### 1.2.3 Execution Orchestration Layer

- (1) Agent Loop: `moltbook_agent_loop()` – Manages turn-based execution of tool calls, up to a configurable maximum (8 turns)
- (2) Task Orchestration: Enforces the predefined sequence (auth → subscribe → upvote → comment)
- (3) Error Handling: Stops execution immediately on any task failure and returns actionable error messages
- (4) Logging System: `log()` function with timestamping and section categorization for auditability
- (5) Homework Wrapper: `run_ft5660_homework()` – Purpose-built entry point for FTEC5660 homework execution

### 1.2.4 Configuration Layer

This layer centralizes all fixed parameters and constants required for agent operation, including the target submolt name, target post ID, Moltbook API base address, and request headers. Centralized configuration makes the agent easy to maintain and modify, and ensures the consistency of task execution targets and API interaction rules.

## 2. Decision Logic and Autonomy Level

### 2.1 Decision Logic Framework

The agent adopts rule-based deterministic decision logic, with all behaviors guided by a pre-defined system prompt and fixed task sequence, without adaptive or creative decision-making. The core execution logic follows an immutable four-step priority sequence:

- (1) Authentication Validation: The mandatory first step. The agent must first verify the validity of the Moltbook API key; all subsequent operations can only be executed if the verification is successful.
- (2) Submolt Subscription: Automatically subscribe to the `ft5660` submolt on the Moltbook platform.
- (3) Target Post Upvote: Execute the upvote operation for the specified fixed post ID according to the homework requirements.
- (4) Target Post Comment: Post a predefined professional English comment to the target post, with fixed comment content to meet the homework specifications.

After the successful completion of all four steps, the agent outputs a fixed success prompt and terminates execution. If any step fails, the agent immediately stops all subsequent operations, records the error details, and returns the error information—there is no retry or alternative action selection logic.

In addition, the decision logic is bound by strict content and behavior rules: no spam, no duplicate content, compliance with platform rate limits, and exact adherence to any human-provided instructions if applicable.

## 2.2 Autonomy Level

The agent is classified as a Level 2 (Assisted Autonomous) agent on a 5-point autonomy scale, with clear autonomy boundaries and no independent decision-making capabilities beyond the predefined scope. The core characteristics of this autonomy level are as follows:

- (1) Full autonomous execution within defined tasks: The agent can complete the pre-set four-step FTEC5660 homework tasks in sequence without any manual intervention, and independently call the corresponding tools according to the logic.
- (2) Zero autonomy beyond the defined scope: The agent cannot create new task goals by itself, cannot modify task parameters (such as target post ID, comment content), and cannot adapt to new or unexpected platform interaction scenarios.
- (3) Minimal error handling autonomy: The agent can detect tool call failures and record detailed error information, but has no self-correction, retry or alternative solution capabilities, and must rely on human intervention to resolve errors.
- (4) No creative content generation: All interactive content (such as comment text) is pre-defined, and the agent has no ability to generate original content according to platform context.

### 3. Moltbook Interactions (Screenshots & Logs)



