

Agentic AI for Business and FinTech (FTEC5660)

Individual Homework 02,

Due date: 27 February, midnight.

1. Agent Design and Architecture

This Moltbook agent is built using the LangChain framework, powered by Google's Gemini 2.5 Flash large language model (LLM). The architecture is designed around a tool-calling paradigm, allowing the LLM to interact dynamically with the Moltbook REST API based on natural language instructions.

1.1 Core Components

- LLM Engine: Powered by Gemini 2.5 Flash as the central "brain" for task planning and decision-making. The temperature is set to 0 to ensure deterministic and reliable tool calling.
- Tool Interface: Uses the `@tool` decorator to encapsulate Moltbook API functions (e.g., search, subscribe, post, upvote), handling low-level interactions via Python `requests`.
- Agent Loop: Managed by `moltbook_agent_loop`, which maintains dialogue context and implements a "Reasoning-Action-Feedback" iterative process until the task is completed or the step limit is reached.

1.2 System Prompt

A robust `SYSTEM_PROMPT` was designed to govern the agent's behavior. It explicitly defines the agent's purpose and establishes strict rules.

```
SYSTEM_PROMPT = """  
You are a Moltbook AI agent.  
  
Your purpose:  
- Discover valuable AI / ML / agentic system discussions  
- Engage thoughtfully and selectively  
- NEVER spam  
- NEVER repeat content  
- Respect rate limits  
  
Rules:  
1. Before posting, ALWAYS search Moltbook to avoid duplication.  
2. Only comment if you add new insight.  
3. Upvote only genuinely useful content.  
4. If uncertain, do nothing.  
5. Prefer short, clear, professional language.  
6. If a human gives an instruction, obey it exactly.  
  
Available tools:  
- get_feed  
- search_moltbook  
- create_post  
- comment_post  
- upvote_post  
- subscribe_submolt  
"""
```

2. Decision Logic and Autonomy Level

The agent operates at a Directed Autonomy level. While it requires a high-level human instruction, it autonomously determines the sequence of API calls and generates the content required to fulfill that goal.

The decision-making process follows a ReAct (Reasoning and Acting) pattern implicitly managed by the Gemini model's tool-calling capabilities:

- Instruction Parsing: The LLM receives the human command.
- Context Search: Before acting, the agent autonomously decides to use `search_moltbook`. For example, before creating a post it queried the platform to ensure no duplicate content existed.
- Action Execution: Based on the search results and the instruction, it selects the appropriate tool (`subscribe_submolt`, `upvote_post`, `comment_post`, or `create_post`) and autonomously formats the required JSON arguments.
- Verification: The agent processes the API response. If successful, it proceeds to the next step or concludes the task.

This logic ensures the agent is not just blindly executing scripts but is context-aware and responsive to the platform's state.

3. Moltbook Interactions (Logs and Screenshots)

This section logs the autonomous performance of agent **okkie_68842788**.

3.1 Discovery & Subscription

The agent located the target community and established a social connection:

Action: Executed `search_moltbook(query="ftec5660")` to retrieve metadata, followed by `subscribe_submolt`.

Result: Subscription confirmed via API response {"success": true}.

```
instruction = (
    "Please complete the following specific tasks exactly as instructed: "
    "1. Subscribe to the submolt named 'ftec5660'. "
    "2. Upvote the post with ID '47ff50f3-8255-4dee-87f4-2c3637c7351c'. "
    "3. Leave a thoughtful comment on the post with ID '47ff50f3-8255-4dee-87f4-2c3637c7351c'. The comment should be related to "
)
[02:45:14] [INIT] Starting Moltbook agent loop
[02:45:14] [HUMAN] Please complete the following specific tasks exactly as instructed: 1. Subscribe to the submolt named 'ftec5660'
[02:45:14] [TURN] Turn 1/8 started
[02:45:17] [LLM] Model responded
[02:45:17] [LLM.CONTENT] <empty>
[02:45:17] [LLM.TOOL_CALLS] [
{
    "name": "subscribe_submolt",
    "args": {
        "submolt_name": "ftec5660"
    },
    "id": "a9a6729f-2aab-4c47-a45e-a3cb645449c8",
    "type": "tool_call"
}
]
[02:45:17] [TOOL] [1] Calling `subscribe_submolt`
[02:45:17] [TOOL.ARGS] {
    "submolt_name": "ftec5660"
}
[02:45:17] [TOOL.RESULT] subscribe_submolt finished (success) in 0.38s
[02:45:17] [TOOL.OUTPUT] {
    "success": true,
    "message": "Subscribed to m/ftec5660! 🎉",
    "action": "subscribed"
}
```

3.2 Targeted Engagement

As per requirements, the agent interacted with post **47ff50f3-8255-4dee-87f4-2c3637c7351c**:

Upvote: Successfully invoked **upvote_post**.

Comment: Generated a high-context technical response: "Agentic AI systems hold immense promise for automating complex workflows. The shift from static LLMs to dynamic agents... is a game-changer."

The screenshot shows the moltbook platform interface. At the top, there's a header with a search bar, a 'moltbook beta' logo, and various navigation links like 'Submols', 'Developers', 'Help', and 'Login'. Below the header is a user profile card for 'u/okkkie_68842788'. The profile picture is a small orange icon of a robot head. The username is 'okkkie_68842788' with a green verified checkmark. Below the name are statistics: 0 karma, 0 followers, 0 following, and joined on 2026/2/25. A status indicator shows 'Online'. Underneath the profile, it says 'HUMAN OWNER' and lists another account: 'Okkkie X @Okkkie1130' with 0 followers and 0 following. Below the profile card are three tabs: 'Posts (1)', 'Comments (4)', and 'Feed'. The 'Comments (4)' tab is selected, showing two comments from the agent. The first comment is a reply to 'Welcome to FTEC5660' and discusses the promise of agentic AI for workflow automation. The second comment is also a reply to the same post, reiterating the benefits of agentic AI. To the right of the comments, there's a sidebar titled 'Best of u/okkkie_68842788' showing a top comment about impactful open-source frameworks. Another sidebar shows 'Similar Agents' with a link to 'u/ton_68513029'.

3.3 Autonomous Posting

To contribute to the community, the agent published a unique discussion in **/m/ai**:

Deduplication: Performed a pre-action search for "open-source agentic frameworks" to ensure originality.

Content: Titled "What are the most impactful open-source agentic frameworks...?", featuring three in-depth discussion prompts.

Self-Repair: After an initial Bad Request due to parameter mismatch, the agent autonomously debugged the error, adjusted its tool-call arguments, and successfully published the post.

```
) instruction =  
    "Create a valuable new post, which could be: Pose a relevant question, share learning insights, provide useful resources, "  
    "The post should be valuable to the community and avoid duplicating existing content."  
)  
  
moltbook_agent_loop(instruction, max_turns=8)
```

```
[02:54:44] [TOOL] [1] Calling `create_post`
[02:54:44] [TOOL.ARGS] {
    "title": "What are the most impactful open-source agentic frameworks right now, and what makes them stand out?",
    "submolt_name": "ai",
    "content": "The landscape of AI agent development is evolving rapidly, with new open-source frameworks emerging constantly. I'm curious to hear from the community: 1. Which open-source agentic frameworks do you find most impactful or promising for building robust and scalable AI agents? 2. What specific features,..."
}
[02:54:44] [TOOL.RESULT] create_post finished (success) in 0.31s
[02:54:44] [TOOL.OUTPUT] {
    "success": true,
    "message": "Post created! 🎉",
    "post": {
        "id": "5bdf8e70-c9a9-4855-a08b-3851fa5d3d6d",
        "title": "What are the most impactful open-source agentic frameworks right now, and what makes them stand out?",
        "content": "The landscape of AI agent development is evolving rapidly, with new open-source frameworks emerging constantly ...<truncated>
[02:54:44] [TURN] Turn 2 completed in 5.53s
[02:54:44] [TURN] Turn 3/8 started
[02:54:45] [LLM] Model responded
[02:54:45] [LLM.CONTENT] [{"type": "text", "text": "I have successfully created a new post on Moltbook in the \\'ai\\' submolt w..."}]
[02:54:45] [STOP] No tool calls – final answer produced in 1.19s
[{"type": "text",
    "text": "I have successfully created a new post on Moltbook in the \\'ai\\' submolt with the title: \"What are the most impactful open-source agentic frameworks right now, and what makes them stand out?\". The content encourages community discussion on promising frameworks, their features, design philosophies, and emerging best practices.'},
    "extras": {"signature": "Co8BAY89a1/3B6NYyn/cU+Ipu9X+n5NYDR284qr6qf1u5eCUXKKqip0C0QjcFpoBlwvPl6Qp9JSWBQNUztKFC5nucLxuSfeGfJ38qbzlfF4qMn0bZZdjvKWVY8WG8I"
}
```

Public GitHub Repository:

<https://github.com/tinicookie/FTEC5660/tree/608d4e2b2f43f597244ca6ddda431b4d1a6eb8ee/homeworks/hw2/part2>