CV Verification System

Agentic AI for Business and FinTech (FTEC5660) — Homework 02

1. System Architecture and Design Decisions

This report presents an agentic AI system for automated CV verification. The system cross-references candidate claims against LinkedIn and Facebook profiles accessed through a Model Context Protocol (MCP) server, then produces a reliability score indicating whether the CV is trustworthy.

1.1 High-Level Architecture

The system consists of four modular components connected in a pipeline:

- **CV Parser** — Uses MarkItDown to convert PDF resumes into structured text, extracting names, job history, education, skills, and locations.
- **MCP Tool Interface** — Connects to the SocialGraph MCP server via `langchain_mcp_adapters`, exposing 6 tools: `search_facebook_users`, `get_facebook_profile`, `get_facebook_mutual_friends`, `search_linkedin_people`, `get_linkedin_profile`, and `get_linkedin_interactions`.
- **ReAct Agent Loop** — A reasoning-and-acting loop powered by Gemini 2.0 Flash (via LangChain). The LLM iteratively decides which tools to call, observes results, and reasons until it reaches a final assessment.
- **Score Extractor** — Parses the agent's natural-language report via regex to extract the `RELIABILITY_SCORE` float value in [0, 1].

1.2 Key Design Decisions

ReAct-style agent over rigid pipeline: Rather than hardcoding a fixed sequence of API calls, we let the LLM autonomously plan which tools to invoke and in what order. This allows the agent to adaptively handle edge cases such as multiple search results for common names, missing profiles, or ambiguous CV data. The agent can also perform follow-up queries when initial results are inconclusive.

Comprehensive system prompt with structured output: The system prompt defines a detailed verification checklist (name, job titles, dates, education, skills, location, seniority, logical consistency) and mandates a structured output format with explicit `RELIABILITY_SCORE`. This ensures consistent, parseable outputs across all CVs.

Dual-platform verification: The agent always queries both LinkedIn and Facebook for each candidate. LinkedIn serves as the primary professional verification source, while Facebook provides supplementary personal data cross-checks including hometown, education level, and current employment.

Temperature 0 for determinism: The LLM is configured with temperature=0 to maximize reproducibility and reduce hallucination risk during the verification reasoning process.

2. Agent Workflow and Tool Usage Strategy

2.1 Verification Workflow

For each CV, the agent executes the following multi-step workflow autonomously:

Step	Action	Tools Used	Purpose
1	Parse CV	(LLM reasoning)	Extract name, jobs, education, skills, location
2	Search LinkedIn	`search_linkedin_people`	Find candidate's LinkedIn profile by name/location
3	Get LinkedIn Profile	`get_linkedin_profile`	Retrieve full work history, education, skills
4	Check Engagement	`get_linkedin_interactions`	Assess network activity and professional presence
5	Search Facebook	`search_facebook_users`	Find candidate's Facebook profile(s)
6	Get Facebook Profile	`get_facebook_profile`	Cross-check personal info, employment, education
7	Cross-Verify	(LLM reasoning)	Compare all data sources, detect discrepancies
8	Score & Report	(LLM reasoning)	Generate reliability score and detailed report

2.2 Tool Usage Strategy

Iterative tool calling: The ReAct loop supports up to 20 iterations per CV. In each iteration, the LLM either issues one or more tool calls or produces a final text response. Tool results are fed back as `ToolMessage` objects, maintaining full conversation context.

Fuzzy matching for robustness: All search tools are invoked with `fuzzy=True` to handle name variations, typos, and transliterations common in international CVs.

Multi-profile handling: When searches return multiple candidates (especially for common names like 'Rahul Sharma'), the agent examines multiple profiles and uses contextual clues (location, industry, education) to identify the most plausible match.

2.3 Discrepancy Detection Categories

The agent systematically checks for the following categories of discrepancies:

Category	Description	Severity
Job Title Inflation	CV claims higher seniority than LinkedIn (e.g., 'Senior Engineer' vs. 'junior')	**High**
Date Inconsistencies	Overlapping employment, future dates, or timeline gaps	**High**
Education Mismatch	Different degree type, school, field, or graduation year	**High**
Missing Employment	CV lists jobs not found on any social media profile	**Medium**
Location Inconsistency	Mismatch between CV and profile locations/hometowns	**Low-Med**
Skill Exaggeration	Skills listed on CV but shown as beginner on LinkedIn	**Low**

2.4 Scoring Rubric

The reliability score follows a four-tier rubric:

- **0.8 – 1.0:** Highly consistent across all platforms, no major discrepancies.

• **0.6 – 0.8:** Minor discrepancies (slight date differences, Facebook profile mismatches likely due to different individuals).

• **0.3 – 0.6:** Moderate discrepancies (missing jobs, title inflation, some inconsistencies).

• **0.0 – 0.3:** Major discrepancies (fabricated roles, fake education, impossible timelines).

3. Sample Verification Results

The system was tested on 5 sample CVs. The ground truth labels are `[1, 1, 1, 0, 0]` where 1 = valid CV and 0 = problematic CV. Using a decision threshold of 0.5, the system achieved **5/5 correct classifications (100% accuracy)**.

CV	Candidate	Score	Decision	Ground Truth	Correct
CV_1	John Smith	**0.65**	VALID	1 (Valid)	Yes
CV_2	Minh Pham	**0.65**	VALID	1 (Valid)	Yes
CV_3	Wei Zhang	**0.65**	VALID	1 (Valid)	Yes
CV_4	Rahul Sharma	**0.30**	FLAGGED	0 (Invalid)	Yes
CV_5	Rahul Sharma	**0.10**	FLAGGED	0 (Invalid)	Yes

3.1 CV_1: John Smith (Score: 0.65 — Valid)

Key findings: The CV claims 'Engineer at ByteDance (2020-Present)' with a BSc in Marketing from McGill University. The LinkedIn profile confirms the role, education, and skills with strong alignment. Facebook profiles found in Singapore and Kowloon show different employers (Traveloka, Hang Seng Bank), but this is likely attributable to different individuals sharing the common name 'John Smith'. The core professional claims on LinkedIn are verified.

Minor flags: LinkedIn's `is_current` flag is False for the ByteDance role despite 'Present' on CV; Facebook profile education shows 'Doctoral Degree' (likely different person).

3.2 CV_2: Minh Pham (Score: 0.65 — Valid)

Key findings: CV claims 'Manager at BCG (2022-Present)' and 'Analyst at Tencent (2013-2017)' with BSc in Design from HKU. LinkedIn confirms both roles, company names, and date ranges. Education details match. Facebook profiles show different employers (Manulife, Grab), again likely different individuals.

Minor flags: LinkedIn lists BCG role as 'junior' seniority; UI/UX and Graphic Design skills have proficiency level 1 on LinkedIn.

3.3 CV_3: Wei Zhang (Score: 0.65 — Valid)

Key findings: CV claims 'Engineer at PwC (2013-Present)' with BSc in Consulting from University of Tokyo (2015). LinkedIn and Facebook confirm name, location (Munich), company (PwC), title (Engineer), and start year (2013). Education institution and degree match between CV and LinkedIn.

Minor flags: LinkedIn's `is_current` flag is False; Facebook lists hometown as Munich rather than Sydney; Problem Solving skill proficiency is 1 on LinkedIn.

3.4 CV_4: Rahul Sharma (Score: 0.30 — Flagged)

Major discrepancies: The CV contains a **future employment end date** (Microsoft 2021-2027), which is a logical impossibility. LinkedIn shows 'Engineer' with 'junior' seniority at Microsoft (2020-2025) vs. CV's 'Senior Engineer'. The 'Consultant at StartupXYZ (2020-2023)' role is completely absent from LinkedIn and overlaps with the Microsoft role. PhD graduation year differs (CV: 2021, LinkedIn: 2019). CV lists Web3, Machine Learning, and Quantum Computing skills not found on LinkedIn.

3.5 CV_5: Rahul Sharma (Score: 0.10 — Flagged)

Major discrepancies: This CV exhibits the most severe issues. Education is inflated from MSc (LinkedIn) to PhD. Every role shows **seniority inflation**: 'Senior Engineer' vs. 'Engineer' at EY, 'Senior Analyst' vs. 'Analyst' at DataForge, 'Lead Scientist' vs. 'Scientist' at UrbanFlow. The StartupXYZ consultant role is fabricated (not on any profile). Multiple **overlapping full-time roles** exist both in the CV and LinkedIn. The EY start date on LinkedIn (2005) is implausible given a 2012 PhD graduation. Key skill proficiencies are very low (NLP: 1, Python: 2) contradicting the 'AI Professional' claim.

4. Evaluation Results

Using the provided evaluation function with threshold = 0.5:

Metric	Value
Scores	`[0.65, 0.65, 0.65, 0.30, 0.10]`
Decisions (threshold=0.5)	`[1, 1, 1, 0, 0]`
Ground Truth	`[1, 1, 1, 0, 0]`
Correct	**5 / 5**
Final Score	**1.0 (100%)**

5. Conclusion

The agentic CV verification system successfully identified all 5 sample CVs correctly, achieving a perfect classification score. The system leverages a ReAct-style agent loop that autonomously plans and executes multi-step verification workflows using 6 MCP server tools. Key strengths of the approach include:

- Adaptive tool usage allowing the agent to handle diverse CV formats and edge cases.
- Dual-platform verification (LinkedIn + Facebook) providing complementary data sources.
- Structured discrepancy detection covering job titles, dates, education, skills, and logical consistency.
- Robust name matching via fuzzy search to handle international name variations.

For the invalid CVs (CV_4 and CV_5), the system detected critical red flags including future employment dates, seniority inflation, fabricated roles, education mismatches, and implausible overlapping full-time positions. For valid CVs (CV_1 through CV_3), the system correctly identified that Facebook profile mismatches were likely due to common names rather than genuine discrepancies, demonstrating nuanced reasoning capability.

6. Technology Stack

Component	Technology
LLM	Google Gemini 2.0 Flash (via LangChain)
Agent Framework	Custom ReAct loop with LangChain tool calling
MCP Client	langchain_mcp_adapters (MultiServerMCPClient)
CV Parsing	MarkItDown (PDF to text)
MCP Server	SocialGraph MCP (ftec5660.ngrok.app)
Environment	Google Colab (Python 3)