

AGENTIC AI SYSTEMS APPLIED TO TASKS IN FINANCIAL SERVICES: MODELING AND MODEL RISK MANAGEMENT CREWS

IZUNNA OKPALA^{*,†}, ASHKAN GOLGOON^{*,‡}, ARJUN RAVI KANNAN^{*,§}

ABSTRACT. The advent of large language models has ushered in a new era of agentic systems, where artificial intelligence programs exhibit remarkable autonomous decision-making capabilities across diverse domains. This paper explores agentic system workflows in the financial services industry. In particular, we build agentic crews that can effectively collaborate to perform complex modeling and model risk management (MRM) tasks. The modeling crew consists of a manager and multiple agents who perform specific tasks such as exploratory data analysis, feature engineering, model selection, hyperparameter tuning, model training, model evaluation, and writing documentation. The MRM crew consists of a manager along with specialized agents who perform tasks such as checking compliance of modeling documentation, model replication, conceptual soundness, analysis of outcomes, and writing documentation. We demonstrate the effectiveness and robustness of modeling and MRM crews by presenting a series of numerical examples applied to credit card fraud detection, credit card approval, and portfolio credit risk modeling datasets.

Keywords:: Large Language Models (LLMs), Multi-Agent Systems, Agentic Systems, Multi-Agent Debate, Multi-Agent Collaboration.

1. INTRODUCTION

Large language models (LLMs) have emerged as a powerful tool in natural language processing, capable of generating and understanding textual data that mimic human behavior. One of the interesting applications of LLMs is their ability to engage in role-playing, where they can simulate various personas, perspectives, or even multiple roles within a conversation [46, 44, 8, 50]. Multi-agent systems leverage the phenomenal role-playing abilities of individual LLM agents through effective debate and collaboration to perform complex tasks and achieve shared goals [6, 54, 76, 44, 31, 20, 13]. Such tasks often surpass what a single highly capable LLM agent can accomplish [6, 13].

Recent research in LLM multi-agent systems has demonstrated considerable potential by equipping collaborative agents with specialized tools, resulting in advanced problem-solving skills in different domains [66, 30].

Multi-agent systems have made great leaps in simulating human-like decision-making processes [68, 55, 35, 44, 12, 8]. Recently, [44] introduced agents that can simulate emergent social behavior. The so-called *generative agents* can initiate and engage in conversations, notice each other, and form opinions. Generative agents are enabled through an architecture that consists of three components, namely *memory stream*, *reflection*, and *planning*. The memory stream records a long-term memory of the agent’s experiences, which,

Date: February 2025.

^{*}Emerging Capabilities Research Group, Discover Financial Services Inc., Riverwoods, IL 60015, USA.

[†] Corresponding author, izunna.okpala@yahoo.com.

[‡] ashkangolgoon@gmail.com.

[§] arjun.kannan@gmail.com.

along with a memory retrieval module, affects the agent’s real-time behavior. To better guide its behavior, the agent utilizes the reflection module, enabling the agent to draw conclusions about others and itself by gradually integrating relevant memories into higher-level inferences. Finally, the planning module is a mechanism that translates an agent’s reflections and current environment variables into action plans, which in turn affect the agent’s behavior in the future.

In the field of software development, [46] proposed a framework known as ChatDev. This framework utilizes LLM-powered (software) agents through natural language communication such that they actively contribute to different phases of software development, namely the design, coding, testing, and documenting stages. ChatDev applies two main mechanisms — the *chat chain* mechanism divides tasks into smaller subtasks to promote seamless collaboration, while the *communicative dehallucination* mechanism tries to minimize coding hallucination. The success of this framework demonstrates how natural language communication can enable agents to effectively collaborate on complex tasks such as software development. Similar examples of agent-based systems for software engineering tasks include code review automation [55], code search and improvement [78], agile development [41], code testing and analysis [63, 39, 17], large-scale software development tasks [47], and code repository generation and navigation [74, 37]. See [14] for a recent review of LLM multi-agent systems applied to software development.

LLM-based multi-agents have been used in various non-conventional yet interesting contexts in a host of different fields. Some of these efforts include synthetic data generation [38, 36], machine translation [66], jury trial and court simulation [7, 53], and healthcare [52, 33, 43, 60].

TransAgents [66] is a multi-agent virtual company that mirrors the translation process in literary texts. This framework possesses a diverse array of roles such as *Senior Editors*, *junior editors*, *translators*, *localization specialists*, and *proofreaders*. For each distinct role, a set of agents is generated to improve the efficiency of the simulations. Moreover, two agent collaboration strategies are examined, namely *Addition-by-Subtraction Collaboration* and *Trilateral Collaboration*. In the debate-style collaboration strategy [35, 12, 6], multiple agents suggest their answers, and a moderator agent wraps up the conversations. Addition-by-Subtraction [66], however, only involves two agents. The *Addition* agent extracts the most comprehensive information possible, while the *Subtraction* agent eliminates redundancies in the extracted information and provides feedback to the Addition agent. The collaboration in the Trilateral strategy is divided into three branches, each assigned to its distinctive agent, namely *Action agent*, *Critique agent*, and *Judge agent*. The Action agent is tasked with following instructions and executing the actions needed. The Critique agent reviews the actions and provides feedback to the Action agent. The Judge agent checks the responses for further revisions and makes the final decision.

Recent progress in LLMs integration with multi-agent systems has opened up groundbreaking opportunities for its application in financial services [42, 27, 79, 3]. Several key streams of research utilizing agentic systems in finance include trading and investment agents [62, 34, 73, 71, 77, 75, 61, 72, 18], markets and economic activities simulation [32, 15, 80, 57], financial sentiment analysis [69], auditing and compliance automation [59, 19], anomaly detection [45], and stock predictions [28].

Generative Pre-trained Transformers (GPTs) do not exactly mimic how human memory works, which is organized into long, medium, and short-term levels. This can make it hard for LLMs to quickly focus on urgent and important tasks such as stock trading, where it is crucial to extract key insights from layered financial data. TradingGPT [34] introduces an LLM multi-agent system with layered memories utilized for stock and fund trading. In this framework, inspired by the hierarchical nature of human memory, an agent assigns perceived memory into *long-term*, *middle-term*, or *short-term* memory layers. Improving on [44]’s metrics for *recency*, *relevancy*, and *importance*, [34] models a hierarchical arrangement of events within each

memory layer and within an agent’s memory. Their treatment of an agent’s memory enables the agents to effectively debate, form strategies, track financial changes, and make informed investment decisions based on their individual risk appetite.

StockAgent [75], another LLM-based multi-agent system, is designed to model investors’ trading behavior in the stock market. The simulations performed using StockAgent are devoted to observing how agent decision-making strategies can influence volatility and liquidity as market indicators. In doing so, simulations are designed to replicate real-world conditions based on NASDAQ and Hong Kong Stock Exchange mechanisms, using two anonymized U.S. stocks, one existing and the other one in the IPO stage.

When it comes to quantitative investment, [62, 73] proposed frameworks known as Alpha-GPT and Alpha-GPT 2.0, respectively. Alpha-GPT [62] introduces a novel approach to quantitative investment research by integrating human-AI interaction for alpha mining, enabling users to convert natural language trading ideas into structured, actionable alpha factors using LLMs. Alpha-GPT addresses challenges like expression validation and backtesting. Alpha-GPT 2.0 [73] expands on this framework, automating the entire research pipeline through a system of AI agents. These agents manage *alpha mining*, *modeling*, and *analysis*, using machine learning tools for tasks like feature selection and portfolio optimization, enhancing the efficiency and scalability of quantitative research.

Apart from leveraging agentic systems as investment and trading tools, agents have been utilized for conducting simulations in economics. The paper [15] examines how LLMs, like GPT-3, can simulate human-like economic behavior, allowing researchers to conduct virtual economic experiments. These simulations mirror traditional economic studies, offering a scalable, cost-effective tool for testing hypotheses before real-world experiments, though with some limitations regarding data quality and representativeness.

EconAgent [32] introduces a new approach to macroeconomic simulation using LLM-powered multi-agent systems. EconAgent creates agents that can simulate human-like economic behaviors, including decision-making in the labor, consumption, and financial markets. The framework addresses key challenges in macroeconomic simulations, such as agent heterogeneity and the influence of macroeconomic trends. The method also offers adaptability and realistic decision-making, exhibiting improved simulations over traditional models, potentially transforming macroeconomic policy analysis and research.

LLM-based agents can be used to model competition in economic and sociological settings. CompeteAI [80] leverages two types of agents, namely *competitors* (e.g., restaurants) and *judges* (customers), to model *competition*. Competitor agents are tasked with managing resources, adjusting menus, hiring staff, and running advertisements, adapting their strategies based on feedback they receive from judges. Judge agents represent customers with diverse preferences (e.g., dietary restrictions and income level). Judges choose between different competitors based on their respective service quality. Moreover, judge agents provide feedback through ratings and comments that influence future decisions of the competitors (such as modifying menus and changing prices). This configuration enables a realistic simulation of competition, offering insights into adaptive strategies and decision-making processes.

Recently, [69] devised a multi-agent system architecture that combines multiple specialized LLM agents, each focusing on a different aspect of financial sentiment analysis. The agents considered include a *Macro Sentiment Agent*, *Micro Sentiment Agent*, *Event Extraction Agent*, and *Knowledge Reasoning Agent*. These agents work together in a coordinated manner to perform comprehensive financial sentiment analysis. The authors argue that multi-agent systems are well-suited for financial sentiment analysis, as the task requires integrating diverse sources of information and capabilities. The modular and distributed nature of a multi-agent system in their case allows for flexibility and scalability in handling sentiment analysis.

Multi-agent systems were recently used for anomaly detection in financial services as well. The paper [45] presents an LLM-based multi-agent framework for anomaly detection in financial services. Agents are defined for specific tasks, such as *data validation*, *external information gathering*, and *institutional knowledge integration*. These agents collaborate to identify, analyze, and validate financial data anomalies efficiently. This framework enhances accuracy and reduces human involvement, making it useful for real-time monitoring and decision-making in financial markets, where quick and reliable anomaly detection is crucial.

Financial services also benefited from applying agentic systems to compliance and auditing automation tasks. Recently, [59] introduced a dual-agent AI system for structured finance tasks. In this framework, one agent handles document extraction, while the other ensures data accuracy via cross-verification between documents like loan applications and bank statements. This configuration, especially using two agents, improves accuracy (up to 100%) but increases computational costs, although it is still faster and more economical compared to manual review approaches. The system is tested on various open- and closed-source models, including Llama 3 and GPT-4, demonstrating the efficiency of multi-agent frameworks for complex document analysis.

Understanding and monitoring multi-agent LLM systems is crucial because their interactions can amplify biases, leading to unintended behaviors and causing potential harm; hence, it is essential to ensure that agents are built strategically to be fair, safe, and ethical in their application to complex tasks. Next, we point out some of these concerns and potential solutions.

The safety of multi-agent systems is important, especially when it involves the financial services industry, a heavily regulated entity. As [5] would put it, harms in agentic systems lead to systemic and long-range impacts, as well as undermining collective decision-making power. They noted the research on FATE (Fairness, Accountability, Transparency, and Ethics) [1, 65], which suggests that as programmable systems become more agentic, they may amplify biases and inequities, particularly for marginalized groups. Some other challenges, not necessarily related to harm and safety, were elucidated by [13]. These include, but are not limited to, the following: optimizing task planning, managing complex context information, and improving memory management. Identifying the challenges of LLM-powered multi-agent systems and their potential solutions is of paramount importance in ensuring the safety and compliance of agentic systems. Some of these challenges include error handling techniques and/or system failures leading to unpredictable behavior like hallucination, lack of control and oversight over the input variables that shape the decision of the system, induced preference or bias, toxic degeneration, and difficulty assessing how agents reach their conclusions.

LLM agents are viewed as “black boxes” primarily because their decision-making is often opaque [48]. Transparency in AI automation is the foundation for trust, and by extension, machine interpretability and bias control. According to [49], safety concerns range from the use of unproven theories, concepts, or questionable data sources in LLM building blocks to the use of retrieval-augmented systems to pull false information from internet sources. These issues can lead to the agentic system exhibiting discriminatory behavior, thus producing harmful results or offensive content [40]. One of the ways to tackle this issue is the introduction of *human-in-the-loop*. This is the ability for humans to intervene or be a part of the processing capabilities of agentic systems. This approach, when applied properly, will be critical to protecting end-users from biased or incorrect outputs [49]. The behaviors and vulnerabilities of agentic systems arise implicitly from the training data specific to the LLM model used rather than being explicitly programmed [49]. According to [16], humans can provide oversight, feedback, and intervention to prevent the agents from taking harmful actions. Since these agents are not fully transparent, a triadic framework involving human regulation, agent alignment, and an understanding of environmental feedback (agent regulation) is needed to address these safety concerns [56].

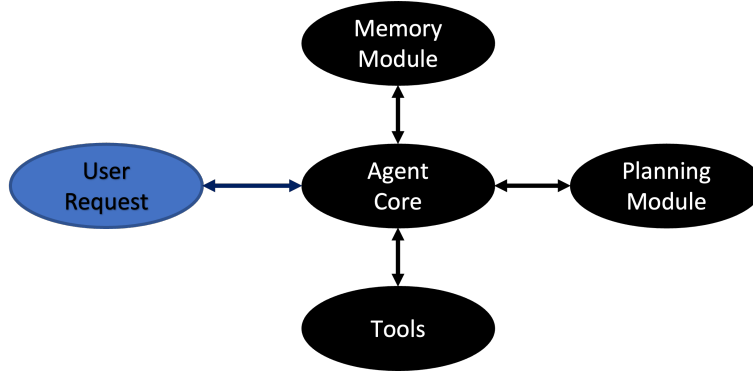


FIGURE 1. General components of an LLM-based agent (adapted from [58])

Another way to tackle the issue of safety and harm in agentic systems is the use of *guardrails*. Guardrails are a set of rules that ensure operational safety and ethical practices in machine learning applications. Their implementation can be in the form of a layered protection model, system prompts, retrieval-augmented generation (RAG) [29] architectures, and other techniques that minimize bias and protect privacy [2]. Guardrails reduce the likelihood of issues like bias, potential for unsafe actions, dataset poisoning, lack of explainability, hallucinations, and non-reproducibility [2]. Moreover, [49] beyond their position on transparency, also argue in favor of guardrails inclusion in LLM-based systems to ensure their runtime behavior is safe and responsible. Ultimately, guardrails are a crucial aspect of harnessing the immense potential of LLMs while minimizing harm and ensuring their alignment with human values.

This paper is organized as follows. In §2, we briefly review the components of agentic systems and agents collaboration strategies. Agentic systems applications in financial services are discussed in §3 with agentic systems for modeling and model risk management workflows, respectively, given in §3.2 and §3.3. Future directions are discussed in §4.

2. AGENTIC SYSTEMS ARCHITECTURES

In this section, we briefly review some important elements of agentic systems architecture and its general components (see [58, 54, 9, 11] for further details).

2.1. Agentic Systems Components. Agentic systems utilize LLMs as their knowledge-bank and are equipped with predefined functions to create a plan for a given task, collaborate with one another, and leverage a wide variety of tools to execute the plan [58]. An agent is typically characterized by the following general components, namely agent core, memory module, tools, and planning module (see Figure 1).

The *agent core* contains information about the core NLP engine (such as GPTs), the agent’s goals, tools, memory, and persona.

The *memory module* consists of short-term and long-term memories. The short-term memory tracks immediate context and actions, while the long-term memory stores information across multiple prior sessions, enabling more personalized interaction to be provided by the agent [58].

Tools are external systems and workflows, APIs, and specialized functions that agents can leverage to perform tasks. These tools allow the agent to interact with the outside world, access real-time data, perform

computations, or control systems. Some examples of agent tools are retrieval-augmented generation (RAG) [29] tools to enable extracting contextually relevant information (context), web browsing and scraping tools, third-party integration tools (e.g., weather, finance, or social media APIs), computation, code execution, and interpreter tools, etc. (see [11, 67, 10, 58]).

In LLM-based agentic systems, a *planning module* is responsible for managing the decision-making and task execution process by breaking down complex tasks into manageable steps. In other words, the planning module acts as a task orchestration engine that manages how an agent handles multi-step, goal-oriented tasks. In doing so, a combination of two techniques, namely task (and question) decomposition as well as reflection (or critique), is used [58]. Task decomposition is used to break down a complex task into smaller (more manageable) subtasks. The reflection or critic mechanism plays a key role in improving the agent’s decision-making, planning, and reasoning processes. Several techniques like *ReAct* [70], *Reflexion* [51], *Chain of Thought* [64], and *Graph of Thought* [4] have emerged as methods for augmenting the planning process by introducing reflective or evidence-based approaches. These techniques enhance the agent’s reasoning capabilities by enabling it to reflect on its own actions, evaluate possible outcomes, and refine its execution plans, resulting in handling tasks with greater accuracy and efficiency.

One should note that there is no general consensus about the definition of agent components in the literature. Next, we focus on CrewAI [11, 10] for defining agent components, as this is the framework we adopt to implement our crews for the rest of the paper. In CrewAI, the key components comprising the agent are *Role Playing*, *Focus*, *Tools*, *Cooperation*, *Guardrails*, and *Memory*.

The memory system in CrewAI helps agents to recall, reason, and effectively learn from past events and interactions [11]. The memory system consists of *short-term* memory, *long-term* memory, *entity* memory, and *contextual* memory. *Role playing* is a specific identity assigned to an agent within the CrewAI system. This provides context and direction, influencing how the agent interacts with other agents and tools. The *Focus* component gives the agent the ability to concentrate on its assigned tasks without being distracted by irrelevant information or activities [10]. The agent is thus able to execute its prompts, enabling the prioritization of its efforts on specific tasks. It connects to the role-playing component, which streamlines the agent to a particular function irrespective of the prompts within the agent’s construct.

For agents to work effectively, especially when there are specialized actions like exploratory data analysis that need to be performed, *tools* are used [11]. *Tools* are the capabilities that agents can utilize to accomplish specific tasks. The selection of appropriate tools is vital, as providing agents with too many options can lead to confusion and inefficiency. *Guardrails* are safety measures and protocols implemented to ensure that agents operate reliably and ethically. These guidelines help prevent issues such as hallucinations (incorrect outputs) and ensure that agents adhere to best practices during their interactions [10]. The component that drives this action is the temperature parameter with the LLM definition. A temperature setting of ‘1’ allows the LLM greater freedom to generate creative or less accurate responses, whereas a temperature of ‘0’ restricts it to deterministic outputs, eliminating such flexibility. It is always a good practice to evaluate trade-offs to ensure agents perform optimally. In our case, we selected a moderate temperature of ‘0.3’ to balance creativity and precision. The *Cooperation* component is arguably one function that makes CrewAI unique. It involves the collaborative efforts of multiple agents working together to achieve common goals. Agents can share information, delegate tasks, and provide feedback to one another, enhancing the overall effectiveness of the system [10].

2.2. Collaboration Strategies in Agentic Systems. Collaboration in agentic systems enables agents to assist one another by sharing information and integrating their skills. In CrewAI [11], this collaboration is realized utilizing *information sharing*, *task assistance*, and *resource allocation*. Effective information sharing

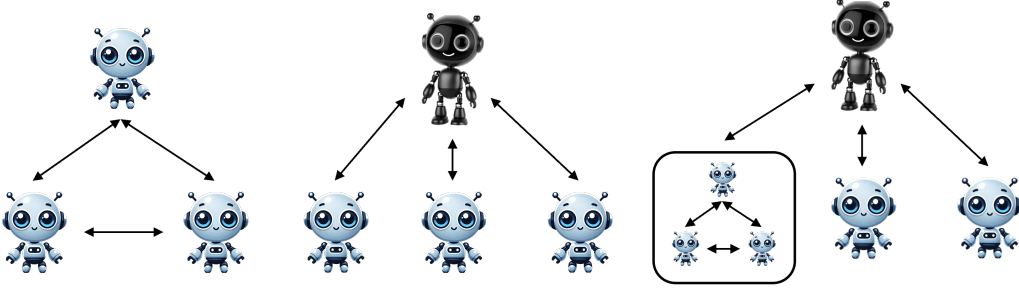


FIGURE 2. Agentic system collaboration structure: Horizontal Collaboration (*left*), Hierarchical Collaboration (*middle*), Nested Collaboration (*right*) (adapted from [13])

is essential to ensure that all agents can communicate their findings and stay well-informed. Task assistance provides the opportunity for agents to ask for help from other agents that possess specialized skills for a task. Finally, resource allocation is responsible for the efficient allocation of computational resources among agents to optimize task execution.

There are multiple collaboration structures in a multi-agent framework based on agents functionality and their interactions, such as *equi-level or horizontal collaboration*, *hierarchical or vertical collaboration*, and *hybrid or nested collaboration* [13, 67, 66] (see Figure 2). In horizontal collaboration, each agent has its own role and strategy, with no agents having a hierarchical advantage over the others. Agents with similar goals collaborate, while agents with opposing goals negotiate or debate to collectively make decisions and complete the task [13]. In a hierarchical structure, a leader agent guides the follower agents to execute its instructions [13]. When both horizontal and vertical structures are present, a nested structure (or hybrid) is formed. Finally, the state of multi-agent systems, their collaboration strategy, agent roles, the number of agents, and their relations may evolve [13]. This scenario leads to *dynamic structures* in which agents may possess dynamically evolving configurations in order to adaptively react to external factors or dynamic conditions [54, 13].

3. APPLICATIONS TO FINANCIAL SERVICES

In this section, we provide an end-to-end agentic system implementation for two major functions in financial services. In particular, we build *modeling* and *model risk management* crews and illustrate how these agents collaborate to perform their specialized collective tasks.

The financial services industry is highly dependent on accurate modeling procedures for its predictive and decision-making capabilities. We develop the modeling and model risk management crews to illustrate how the agents can collaborate to perform relatively complex functions in an efficient and scalable manner. The goal is to streamline the modeling workflow, carry out model risk management procedures on a trained model, and effectively manage dependencies as well as collaboration among agents.

The system architecture for the financial crews, along with the memory property and role-playing, are discussed in §3.1. Agentic workflows for modeling and model risk management crews are discussed in §3.2 and §3.3, respectively. We provide three modeling use cases to highlight the diverse range of tasks that can be accomplished with agentic systems, namely *credit card fraud detection*, *credit card approval*, and *portfolio credit risk modeling* in §3.4. We initialize all agents with GPT-3.5 Turbo from OpenAI as the underlying

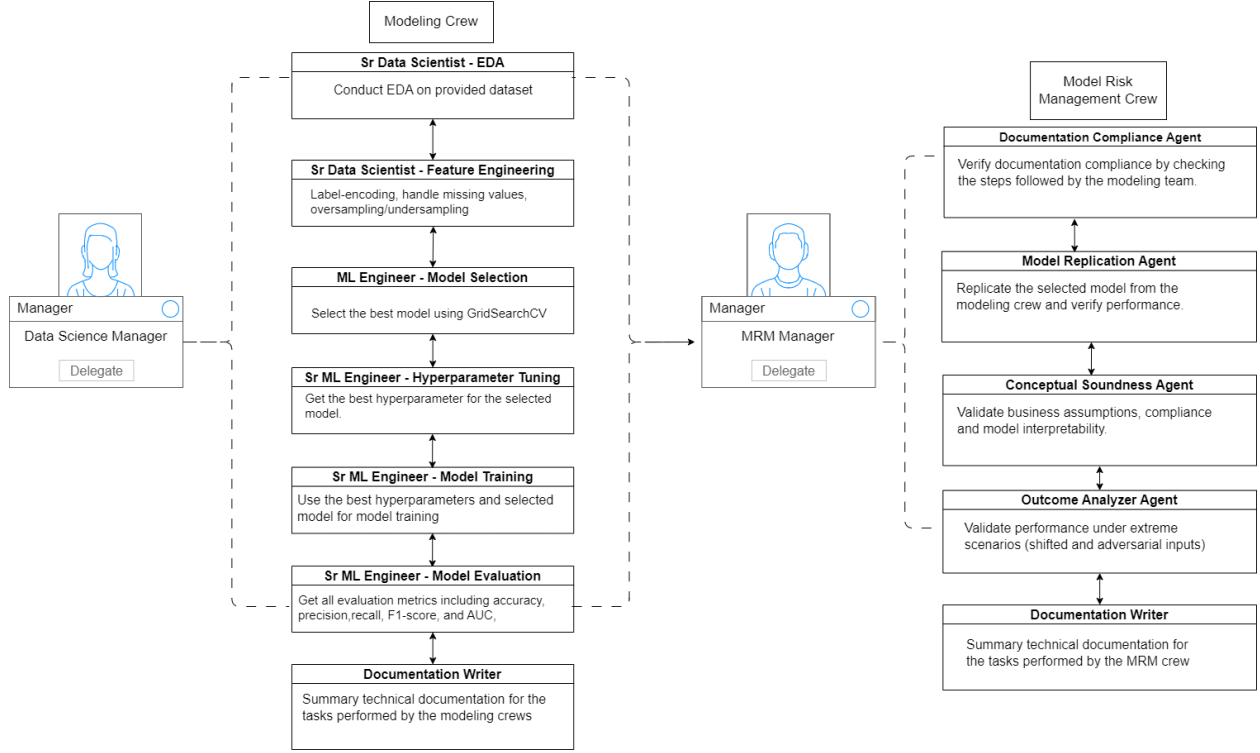


FIGURE 3. Full system architecture for the modeling and model risk management crews

large language model for their individual and coordinated tasks. CrewAI serves as the foundational platform for managing the agentic systems illustrated in this paper.

3.1. Financial crews system architecture. The proposed system comprises two interconnected crews and tools. Within the crews, we have several autonomous agents, each responsible for distinct tasks within the pipeline. The architecture is designed to promote modularity, allowing agents to operate independently and collaboratively. The key crews and agents include:

- (1) Modeling Crews
 - Exploratory Data Analysis (EDA)
 - Feature Engineering
 - Model Selection
 - Hyper-parameter tuning
 - Model Training
 - Model Evaluation
 - Documentation Writer
 - Manager
- (2) MRM Crews
 - Documentation Compliance Checker
 - Model Replication

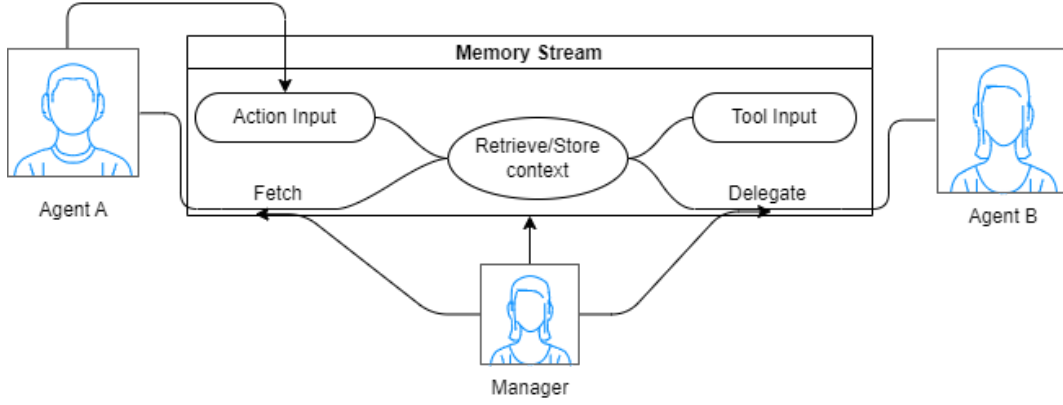


FIGURE 4. Memory, delegation and information retrieval

- Conceptual Soundness
- Outcome Analyzer
- Documentation Writer
- MRM Manager

3.1.1. *Memory, delegation and information retrieval.* The memory property is most effective when individual agents store their inputs and outputs in memory, allowing the manager agent to retrieve them when needed. Since the manager oversees all processes, it can query any agent’s memory for relevant data. These interactions, including inputs and outputs, are visually represented in Figure 4. The memory stream is an object with a specific capacity and can hold task delegations in natural language, task execution timestamps, and the information needed by the collaborating agent. The core attribute of the memory object is its retrieval and storage of interconnected interactions from different agents. For example, let us walk through the responsibilities of one of the agents in the modeling crew and the management of the memory stream. The crew consists of multiple members, each with distinct or overlapping functions. In this section, we will focus on the role of the Senior Data Scientist in charge of the data exploration task (see Figure 5). The Senior Data Scientist conducts exploratory data analysis to observe the following insights and trends over time: (1) shape of the dataset, (2) features with missing values and the percentage of missing values within those features, (3) correlation matrix across multiple features, (4) descriptive statistics for each feature, (5) data distributions, including positive and negative skewness, and (6) outlier or adversarial inputs. The memory stream stores all inputs and outputs and can be queried by the manager to retrieve certain information or actions from the agent as input and pass the same information to the next agent. In this study, we aim to elucidate three key components of the memory stream: tool input, action input (such as generated code), and context.

3.1.2. *Role playing properties of the system.* The “role-playing feature” makes the solution more intuitive, since specific roles or personas are assigned to each agent, guiding their behavior and decision-making within a collaborative task.

These roles represent specific job functions, such as data engineering or machine learning engineering, based on the requirements and objectives of the initialized agents. We briefly touched on the role of the Senior Data Scientist in §3.1.1. There are two Senior Data Scientists (modelers): The goal of the first modeler is

to conduct an in-depth exploratory analysis of the provided data. The second modeler prioritizes feature engineering, with a particular emphasis on addressing data imbalances commonly found in portfolio credit risk, credit card approval, or credit card fraud detection datasets. The third agent is a Machine Learning Engineer with a good understanding of the different strengths and weaknesses of machine learning models, making it a good candidate for model selection. The interdependent functions of the modelers and other agents illustrate the necessity for collaboration and the value of clear and designated roles. The subsequent three agents are all designated as Senior Machine Learning Engineers and are tasked with hyperparameter tuning, training the selected model with optimal hyperparameters, and evaluating its performance. Specifically, the hyperparameter tuning agent is prompted to check the various hyperparameters needed for executing the selected model (e.g., number of trees, maximum depth, learning rate, etc.), tune those hyperparameters with a predefined range of numbers, and get the optimal result (see hyperparameter tuning execution in Appendix A). The model training agent is prompted to use the optimal hyperparameters to train the selected model. Here, the importance of the memory stream is emphasized; different results were chained together to achieve the common goal of the entire crew. The evaluation agent is prompted to evaluate the trained model based on five metrics, namely accuracy, F1-score, recall, precision, and capture rates.

The manager agent, regarded as a pivotal figure, assumes the role of “Data Science Manager,” well-versed in financial modeling. Its primary responsibility is to supervise the entire process, ensuring that all agents and the data used meet specified standards. Additionally, the data science manager provides overarching guidance to prevent deviations from assigned roles and duties.

3.2. Agentic systems for modeling workflow in financial services. The agentic system, introduced in §1, features a modular architecture that leverages the strengths of individual components to achieve a unified goal. Figure 3 provides a more clear description of agentic systems and how tasks are segmented based on expertise. In this section, we discuss the workflow of our proposed agentic system applied to financial modeling. The distinct roles, facilitate specialization (see §3.1.2). We provide detailed descriptions of these agents, their assigned functions, and the methods used to prompt them.

- (1) EDA Agent: This is an instance of the “Agent” class in CrewAI, and it focuses on exploratory data analysis. The “role” parameter specified within the agent’s construct is the “Senior Data Scientist.” As already mentioned in the role-playing properties of an agentic system, this helps establish context and expertise for the agent. This agent includes procedures with a specialized tool, “EDA Tool,” specifically designed to capture the nuances not captured by basic data exploration. This includes identifying missing values, class imbalances, categorical variables, and/or outliers that needs to be addressed. It also shows the data distribution of all the features, capturing skewness and correlation across features. The agent is prompted to identify all the results from the “EDA Tool,” and to show the result in a summarized and easy-to-read format (see Algorithm 1 and Log 1).
- (2) Feature Engineering Agent: This agent performs data transformation using the “Code Execution Tool.” This tool is specifically developed to handle Python code execution. It takes the instance of a Python service offered by the local environment that runs the agentic system. With this capability, an agent can generate a code and pass the code to the tool to run. The feature engineering agent handles missing values, encodes categorical variables, and balances imbalanced datasets depending on the manager’s instructions (see Log 2). We will explore the capabilities of the manager in the “manager agent” description. The feature engineering agent maintained the role of a “Senior Data Scientist” because there are some statistical operations that need to be performed.

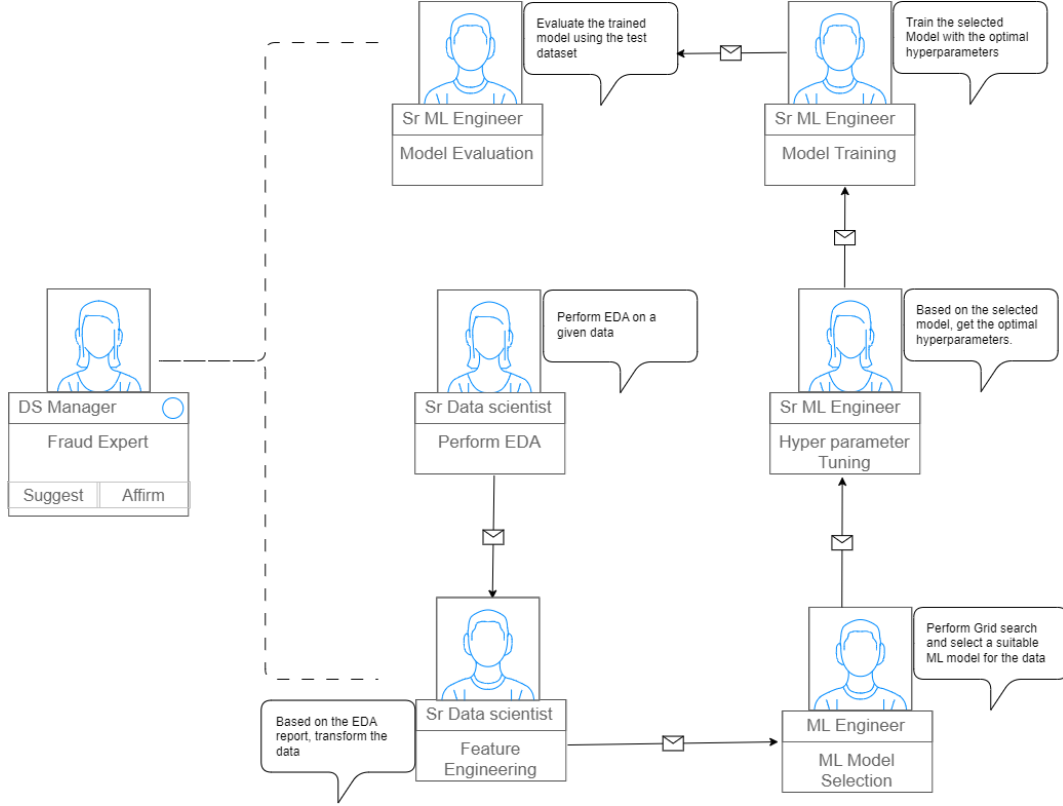


FIGURE 5. Role Playing characteristics of the fraud modeling crews

- (3) **Model Selection Agent:** This agent is configured to select the best model for a given dataset using the GridSearchCV method. Its output is designed to combine the selected model and the rationale behind the selection. It takes the persona of a “Machine Learning Engineer.”
- (4) **Hyperparameter Tuning Agent:** This agent is responsible for finding the best performing hyperparameters for the selected model using the “Code Execution Tool.” The task connected to the agent is configured to find the hyperparameters and save them as a dictionary output. Its “role” is that of a “Senior Machine Learning Engineer,” and it is not allowed to delegate tasks to other agents.
- (5) **Model Training Agent:** This agent is responsible for generating and executing Python code using the “Code Execution Tool,” to train the selected machine learning model using the best hyperparameters from the hyperparameter tuning agent. There is also a provision within the prompt for saving the trained model to a predefined directory. The agent takes the persona of “Senior Machine Learning Engineer.”
- (6) **Model Evaluation Agent:** This agent is responsible for evaluating the trained model using the test data. The generated code calculates the accuracy, F1-score, precision, recall, AUC, and overall performance of the model using the transformed test data from the “Feature Engineering Agent.” This agent takes on the persona of a “Senior Machine Learning Engineer.”
- (7) **Manager Agent:** The manager has specific characteristics. It takes the role of a “Data Science Manager,” with the goal to “manage and delegate subtasks to coworkers.” It oversees other agents’

tasks and gives specific instructions to individual agents on how to handle their functions effectively. Depending on the use case, the manager agent is typically furnished with a strong background in portfolio credit risk, credit card approval, or credit card fraud data science modeling, enabling it to make informed decisions as a subject matter expert in their respective fields.

- (8) **Documentation Writer Agent:** This agent writes a technical documentation for all the tasks performed by the modeling agents. The agent is skilled in technical writing with a deep understanding of data science workflows. It uses the CrewOutput instance to gather all the outputs from the crews to create a comprehensive summary of all the tasks within the agentic ecosystem.

3.3. Agentic systems for model risk management workflow in financial services. The model risk management (MRM) crew can be seen as a safeguard team that ensures the modeling crew is operating as intended while upholding regulatory rules, business objectives, and modeling functions. It features a modular architecture that capitalizes on the strengths of individual components to accomplish a shared objective. Figure 3 offers a more explicit illustration of how the MRM crew interfaces with the modeling crew and the distinct agents involved. We present comprehensive descriptions of MRM agents, their designated functions, and how these agents are prompted.

- (1) **Documentation Compliance Checker:** This agent checks for documentation and procedural compliance. The documentation produced after the modeling crew completes their tasks is verified by this agent using the organizational modeling guide.¹ This guide shows the steps that need to be followed when training or building machine learning models. The agent utilizes Retrieval-Augmented Generation (RAG) framework to compare the steps and tasks handled by the modeling crew with the modeling guide. Since this function includes components that require domain knowledge in data science, it takes the “role” of a “Senior Data Scientist.”
- (2) **Model Replication:** This agent is responsible for thoroughly replicating the model selected and trained by the modeling crew to ensure its performance metrics align with their results. It receives the model’s hyperparameters and name from the modeling crew and replicates the model within its own environment for validation. Its designated role is “Senior Machine Learning Engineer.”
- (3) **Conceptual Soundness:** This agent focuses on comprehensive validation of the trained model through a validated business case, performance benchmarks, interpretability, and model compliance. The “role” parameter specified within the agent’s construct is the “Senior Model Validation Analyst.” This choice helps establish context and expertise for the agent. The agent applies mechanisms to check the model’s robustness, and compliance. The business case in the context of conceptual soundness is the procedure found in the modeling guide, which can differ across organizations. The conceptual soundness function involves a deep dive into the conceptual framework of a particular model, the target objectives, data characteristics, and constraints.
- (4) **Outcome Analyzer:** This agent tests the trained model using transformed data that simulate extreme conditions. These extreme conditions involve regenerating the inputs by multiplication or the addition of some fixed/randomized values, effectively creating adversarial inputs for the model (see Appendix C). The agent is prompted to perturb the test data, leading to simulated shifts in input data distributions and outlier input. These inputs will then be tested on the trained machine learning model to evaluate its robustness. The agent has the role of a “Senior Model Validation Analyst.”

¹This organizational modeling guide is AI-generated and intended for illustrative purposes only. It is not affiliated with, endorsed by, or reflective of the actual internal modeling guide of the Discover Financial Services.

Algorithm 1 Modeling Crew

```

Agent role  $\leftarrow$  Data Science Manager
  goal  $\leftarrow$  Manage the overall modeling pipeline with specific instructions
  backstory  $\leftarrow$  An expert, skilled with managing a modeling team.
  if (agent in [list of agent...]) then
    agent = context(instruction)  $\leftarrow$  manager_instruction
    tool = [eda_tool, code_executor]
  end if
End
Agent
  procedure (EDA) role  $\leftarrow$  Senior Data Scientist
    goal  $\leftarrow$  Conduct a detailed exploratory data analysis
    backstory  $\leftarrow$  EDA expert.
    tool = [eda_tool]
    task  $\leftarrow$  manager_instruction
  end procedure
  procedure (Feature Engineering) role  $\leftarrow$  Senior Data Scientist
    goal  $\leftarrow$  Preprocess the data for model training
    backstory  $\leftarrow$  Skilled Feature Engineer.
    tool = [code_executor]
    task  $\leftarrow$  manager_instruction
  end procedure
  procedure (Model Selection) role  $\leftarrow$  Machine Learning Engineer
    goal  $\leftarrow$  Select the best Machine Learning model
    backstory  $\leftarrow$  Expert in using GridSearch or RandomSearch.
    tool = [code_executor]
    task  $\leftarrow$  manager_instruction
  end procedure
  procedure (Hyperparameter Tuning) role  $\leftarrow$  Sr. Machine Learning Engineer
    goal  $\leftarrow$  Get the optimal hyperparameters for the selected model.
    backstory  $\leftarrow$  Hyperparameter tuning expert.
    tool = [code_executor]
    task  $\leftarrow$  manager_instruction
  end procedure
  procedure (Model Training) role  $\leftarrow$  Sr. Machine Learning Engineer
    goal  $\leftarrow$  Train the selected model with the best performing hyperparameters.
    backstory  $\leftarrow$  Machine learning training expert.
    tool = [code_executor]
    task  $\leftarrow$  manager_instruction
  end procedure
  procedure (Model Evaluation) role  $\leftarrow$  Sr. Machine Learning Engineer
    goal  $\leftarrow$  Evaluate the trained model.
    backstory  $\leftarrow$  Model evaluation expert.
    tool = [code_executor]
    task  $\leftarrow$  manager_instruction
  end procedure
End

```

- (5) Documentation Writer: This agent produces technical documentation similar to that of the modeling crew, and it is skilled in technical writing with a deep understanding of data science workflows.
- (6) MRM Manager: The manager agent is a replica of a manager in the modeling crews discussed. The only difference here is that it has a strong background in model risk management, enabling it to manage the actions of the documentation compliance checker, the conceptual soundness agent and outcome analyzer agents.

Algorithm 2 Model Risk Management Crew

```

Agent role  $\leftarrow$  Model Risk Manager
  goal  $\leftarrow$  Oversee the overall modeling risk management team with specific instructions
  backstory  $\leftarrow$  An expert, skilled in model risk management.
  if (agent in [list of agent...]) then
    agent = context(instruction)  $\leftarrow$  manager_instruction
    tool = [code_executor, RAG]
  end if
End
Agent
  procedure (Documentation Compliance Checker) role  $\leftarrow$  Senior Data Scientist
    goal  $\leftarrow$  Verify the modeling crew documentation for compliance.
    backstory  $\leftarrow$  Experienced compliance checker, for model training.
    tool = [RAG]
  end procedure
  procedure (Model Replication) role  $\leftarrow$  Senior Machine Learning Engineer
    goal  $\leftarrow$  Replicate the model from the modeling crew, and verify results.
    backstory  $\leftarrow$  Experienced independent agent in training and testing a model.
    tool = [code_executor]
  end procedure
  procedure (Conceptual Soundness) role  $\leftarrow$  Senior Model Validation Analyst
    goal  $\leftarrow$  Assess model's assumptions, performance metrics, and interpretability.
    backstory  $\leftarrow$  Experienced agent in validating model assumptions.
    tool = [code_executor]
  end procedure
  procedure (Outcome analyzer) role  $\leftarrow$  Senior Model Validation Analyst
    goal  $\leftarrow$  Perturb the data, and independently check the performance metrics.
    backstory  $\leftarrow$  Skilled independent outcome analyzer.
    tool = [code_executor]
  end procedure
End

```

3.4. Experiments and Results. We conduct agentic experiments involving three practical use cases relevant to the financial services industry. Figure 6 shows the process flow, illustrating how the agentic system operates in conjunction with tasks and tools. Both the modeling and MRM crews adhere to this paradigm. The process, outlined earlier in Algorithm 1, demonstrates a hierarchical process. This gives the manager the ability to delegate and manage the agents and tasks available to them for various functions. The available tools can be utilized by any agent or task based on the manager's directives.

3.4.1. Credit Card Fraud Detection Dataset. We present the performance metrics derived from parsing the credit card fraud detection dataset [21] through the agentic system and highlight several subtleties involved.

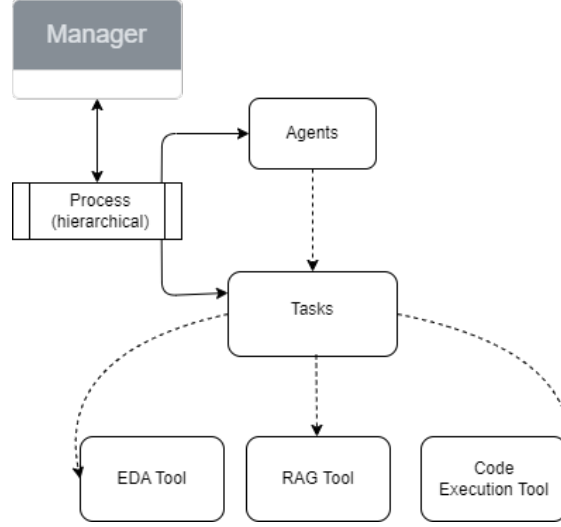


FIGURE 6. Pictorial representation of the Manager-Agent-Task-Tool integration

The dataset contains 284,807 rows and 31 columns. The “Class” column serves as the target variable for binary classification. This column identifies whether a transaction is fraudulent (represented by 1) or non-fraudulent (represented by 0). A notable characteristic of the dataset is its class imbalance, as 99.83% of the transactions were non-fraudulent. Apart from the target feature, the dataset consists entirely of 29 numeric features and a date feature. The numeric feature includes the “Amount” feature, representing the monetary value of each transaction. The remaining 28 features were anonymized, labeled “V1” to “V28.” There were no missing values, categorical, or text-based features. The Data Science Manager, as seen in Algorithm 1, handles the delegation of tasks in the pipeline, making the process hierarchical in nature. The initial task in the pipeline is the exploratory data analysis. This task, with additional instructions from the manager, is handed off to the EDA agent, a Senior Data Scientist. The handoff and execution are found in Log 1. Also, check Appendix A to see a snippet of end-to-end interactions between agents.

LOG 1. Manager - EDA Agent interaction

```

Working Agent: Data Science Manager
Starting Task: Conduct a detailed exploratory data analysis on the provided dataset located
               ↪ at 'fraud_dir/fraud.csv'.
Action: Delegate work to coworker
coworker: "Senior Data Scientist I"
    
```

The model trained via the agentic system prompts presents a good performance when compared to the most upvoted solution on Kaggle [22]. The Kaggle solution addressed class imbalance through random downsampling and oversampling. Their top-performing models with the downsampling method include logistic regression with an accuracy of 94% and an F1-score of 94%. Other models, such as K-Neighbors and Support Vector Classifier, reported similar accuracy levels of 93%. Our agentic solution also utilized logistic regression as the best performing model from the model selection agent, with an accuracy of 94.39%, an F1-score of 94.24%, and a recall of 91.84% (refer to Figure 7). The prompt for the feature engineering agent utilized a **random downsampling** technique due to the overwhelming majority of the data belonging to one class (99.83%), a process guided by the manager’s instruction. This feature engineering step was preceded

by train-test-split using the 80/20 rule to avoid data leakage. The top five performing features using the log odds ratio or the coefficient of the logistic regression function are “V4, V22, V21, V28, and V27.”

The model risk management analysis highlights some crucial points. The model was tested on two inputs; the shifted inputs and outlier inputs. The shifted inputs were derived by randomly assigning new values to non-categorical features, while outliers are generated by taking a feature and increasing it beyond its original distribution range. The shifted input function was applied to all the features primarily because the fraud dataset had no categorical variables. There was a slight decline in performance for the shifted inputs; accuracy dropped from 94.39% to 91.33%, F1-score from 94.24% to 91.79%, and AUC from 94.39% to 91.33%. Although there was a decline, we still had a considerable above average performance indicating the model’s resilience in handling shifted inputs. We can validate this with the model’s performance on outlier or adversarial inputs. The model was able to maintain same performance in adversarial inputs, with accuracy, F1-score and AUC remaining at (94.39%, 94.24%, 94.39% respectively, see Figure 7). This suggests that the model is not overly sensitive to the presence of anomalous instances. An interesting point, not immediately apparent, is that the anonymized features denoted as “V1” to “V28” underwent feature scaling. This scaling process enabled the model to effectively handle shifted inputs and outliers originating from the downsampled test dataset.

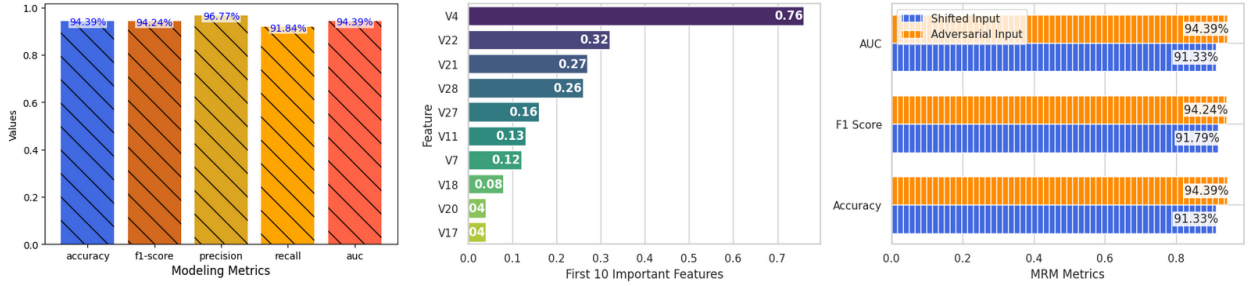


FIGURE 7. Performance report for the Credit Card Fraud Detection dataset

3.4.2. Credit Card Approval Prediction Dataset. This section provides an overview of evaluating the performance of the agentic system when applied to the credit card approval dataset [24]. The dataset consists of two tables: one for application records and the other for credit records. The target variable, “STATUS” is encoded as follows: ‘0’ indicates 1-29 days past due, ‘1’ represents 30-59 days past due, ‘2’ signifies 60-89 days overdue, ‘3’ corresponds to 90-119 days overdue, ‘4’ denotes 120-149 days overdue, ‘5’ stands for accounts that are overdue or classified as bad debts with write-offs for more than 150 days, ‘C’ indicates accounts that were paid off within the month, and ‘X’ signifies that there was no loan activity for the month. For the sake of simplicity, the “STATUS” variable was transformed into binary inputs, where ‘0’, ‘1’, ‘X’, and ‘C’ represents non-default scenarios, and other values represent defaults. The two tables were merged on the “ID” column. Together, they contained 36,457 rows and 20 columns after dropping duplicates. The key numeric features include “CNT_CHILDREN”, “AMT_INCOME_TOTAL”, “DAYS_BIRTH”, “DAYS_EMPLOYED”, and “MONTHS_BALANCE.” The 12 notable categorical features, including numeric features are “CODE_GENDER,” representing gender, “F_OWN_CAR”, denoting whether the person owns a car, and “F_OWN_REALTY”, indicating property ownership. The “N_INCOME_TYPE” feature categorizes income sources, while “N_EDUCATION_TYPE” reflects education level and “N_FAMILY_STATUS,” marital status. Additionally, “N_HOUSING_TYPE” describes living situation, and “OCCUPATION_TYPE” shows occupation. Other categorical indicators include “F_MOBIL,” “F_WORK_PHONE,”

“F_PHONE,” and “F_EMAIL,” denoting the presence of mobile phones, work phones, personal phones, and email addresses, respectively. This dataset in its entirety also has the issue of class imbalance, with 98.31% of the instances belonging to the majority class (“STATUS” = 1). The description in Log 2 illustrates the feature engineering process for the credit card approval use case, which occurs subsequent to the EDA phase. Refer to Appendix A for a sample end-to-end interaction between agents for the credit risk use case.

LOG 2. Manager - Feature Engineering Agent interaction

Working Agent: Data Science Manager

Starting Task: Preprocess the test and train dataset located on 'card/test.csv' and 'card/train.csv' respectively.

- 1) Perform label encoding only on the categorical features with fit_transform and transform methods respectively.
- 2) Use K-Nearest Neighbors (KNN) imputation to fill missing values in the test and train dataset.
- 3) Perform SMOTE Synthetic Minority Over-sampling Technique on the train and test dataset using fit_resample method.
- 4) Save the transformed test and train data in the directory 'card/' as 'test2.csv' and 'train2.csv' respectively.

I need to delegate the feature engineering task to the Senior Data Scientist II to preprocess the test and train datasets as per the given instructions.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Feature Engineering",
  "coworker": "Senior Data Scientist II"
}
```

After the completion of the feature engineering phase, the manager agent follows the steps described in Algorithm 1. The accuracy of the model selected by the agentic system is 95.48%. This performance slightly outperforms the upvoted solution on Kaggle [25]. The Kaggle solution achieved an accuracy of 93.79% with XGBoost. The key metrics reported by the Kaggle solution include a precision of 94.5%, a recall of 92.6%, and an F1-score of 93.5%. In contrast, our solution applied the Random Forest algorithm with precision at 99.45%, recall at 91.47%, and F1-score at 95.30%. These metrics indicate that the model excels at identifying and categorizing credit card approval patterns. The model risk management analysis revealed a slight decline in key metrics, notably under shifted data distributions. Although there was a marginal decrease in accuracy, F1-score, and AUC, indicating a slight performance dip, the model retained its ability to generalize well to unseen inputs. The shift in data distribution specifically targeted non-categorical variables, as categorical variables have fixed values (e.g., ‘YES’ or ‘NO’ for “F_OWN_CAR”), while numerical features like “AMT_INCOME_TOTAL” can vary. Given that most of the features were categorical, the impact on key metrics for both shifted and adversarial inputs were minimal. The top five performing features using the permutation feature importance of the random forest algorithm are “F_OWN_REALTY, CODE_GENDER, ACCOUNT_AGE, F_OWN_CAR, and F_PHONE.”

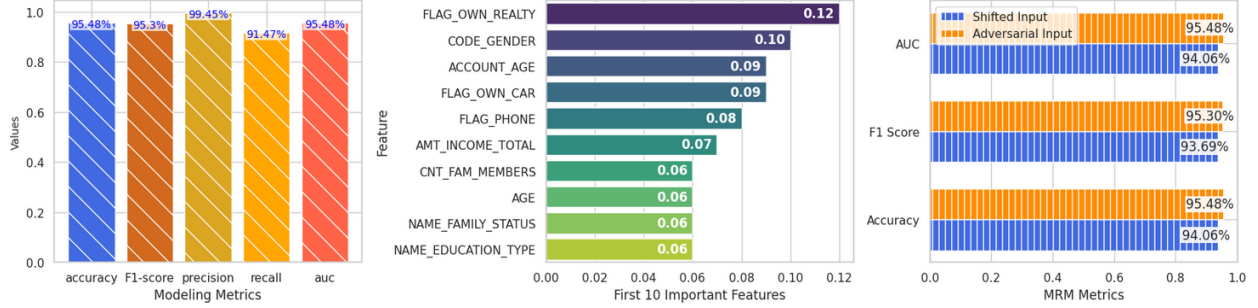


FIGURE 8. Performance report for credit card approval

3.4.3. Portfolio Credit Risk Dataset. The result of using agentic programming on the portfolio credit risk dataset [23] presents further arguments to underscore the importance of model risk management. Refer to Appendix A for a detailed overview of the end-to-end interaction among agents for the portfolio credit risk use case. The dataset [23] contains 32,581 data points and 12 features, with the target feature named “loan_status.” The “person_age” feature indicates the age of the borrower, while “person_income” represents their annual income. The “person_home_ownership” feature describes the borrower’s home ownership status, which can impact their creditworthiness. Additionally, “person_emp_length” reflects the length of employment in years. Loan characteristics are detailed through the “loan_intent” and “loan_grade” features, which outline the purpose of the loan and its associated grading. The “loan_amnt” specifies the total amount borrowed, and “loan_int_rate” provides the interest rate applicable to the loan. The target variable, “loan_status”, indicates whether the loan has defaulted (1) or remained non-default (0). The “loan_percent_income” shows the proportion of income allocated to loan repayments, while “cb_person_default_on_file” reveals historical default records. The “cb_person_cred_hist_length” measures the length of the borrower’s credit history, providing insights into their borrowing behavior.

The credit risk dataset, like the fraud and the card approval dataset also had class imbalance issue, with 78.18% of the instances belonging to the majority class (“loan_status” = 1). Missing values were found on two features: “person_emp_length” (2.75% missing) and “loan_int_rate” (9.56% missing). The preliminary performance metrics demonstrate the robustness of the model trained through collaborative efforts within the agentic system, showcasing an accuracy of 95.37%. This result was slightly above the accuracy recorded by the upvoted solution on Kaggle [26]. The preprocessing section of the Kaggle solution involved the creation of new features including income group, loan amount group, loan-to-income ratio, and interest rate-to-loan amount ratio. They employed OneHotEncoder for categorical variable encoding. Among their top-performing models were CatBoost, exhibiting an accuracy of 93.72%, AUC of 94.32%, recall of 72.68%, precision of 97.78%, and an F1-score of 83.37%, and LightGBM, which achieved an accuracy of 93.54% and an AUC of 94.15%, among others. Conversely, the agentic system employed an XGboost classifier, achieving an accuracy of 95.37%, an AUC of 95.37%, precision of 99.08%, recall of 91.58%, and an F1-score of 95.18%. The feature engineering agent had specific instruction to use LabelEncoding for categorical variable encoding and KNN imputation to fill missing values (see Appendix A). The top five performing features were “loan_grade, loan_percent_income, cb_person_default_on_file, person_home_ownership, and loan_intent.”

Upon further analysis by the MRM crew, a performance decline was identified. For the shifted inputs, accuracy, F1-score, and AUC all experienced reductions, with accuracy dropping to 86.24%, F1-score to 86.92%, and AUC to 86.24%. These findings suggest that the model may be vulnerable to shifts in input data distribution. Compared to the card approval use case, the credit risk dataset contains fewer categorical

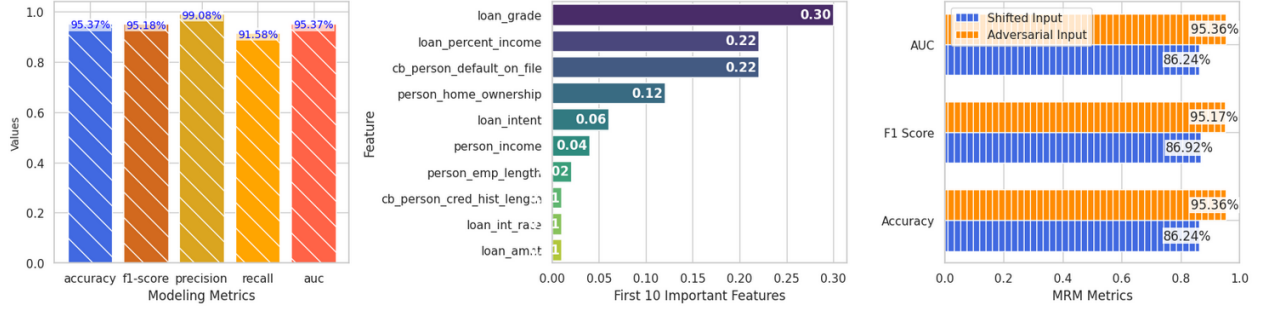


FIGURE 9. Performance report for portfolio credit risk

variables, indicating that a substantial portion of its input data experienced a distribution shift. Additional analysis using adversarial inputs demonstrated the model’s resilience, with accuracy, F1-score, and AUC consistently remaining high at 95.36%, 95.17%, and 95.36%, respectively. This indicates that the model effectively handles and categorizes adversarial cases.

3.4.4. Model Risk Management. Model risk management provides benchmark and safeguard mechanisms beyond adversarial and shifted input tests, as detailed in each experimental result. This critical component of the agentic architecture (see Figure 3) ensures that the modeling crew complies with organizational documentation standards (see Log 4). The oversight of this module is the responsibility of the MRM Manager, who leads the team to verify that the models developed by the modeling team are both compliant and consistent. The “Documentation Compliance Checker Agent,” utilizes the RAG tool to validate each step of the modeling procedure against the organization’s modeling guide. As shown in Log 4, the initial prompt directed the agent to review the modeling documentation and the organization’s modeling guide. This review establishes a baseline to confirm that the modeling team adhered to the prescribed procedures. The log output confirms that the modeling documentation aligns with the organization’s guidelines. The “Model Replication Agent” replicates the training and testing of the selected model with exact hyperparameters used by the modeling crew to verify that their results align. The “Conceptual Soundness Agent” assesses the model’s adherence to business case, evaluates its performance metrics, and verifies its interpretability. Detailed results for these assessments are documented in the log, with specific descriptions provided for each finding. Additional tests were also performed per manager’s request by the “Outcome Analyzer Agent” to simulate extreme scenarios and test the models’ adaptability to change.

3.4.5. Human verification of results - Reliability check. The complexity of the agentic system calls for human evaluation. This is done to make sure that the agents do not produce unreliable outputs and also to determine the usage of the provided dataset. In the case of the modeling and MRM crew, the authors meticulously verified each output and examined the various codes and inferences generated by the agents. By running these outputs side by side in a controlled Python environment, we were able to confirm that the results were consistent and accurate. Not only was accuracy accounted for, but the output was in line with standard machine learning assumptions. This human-centered validation process serves as a crucial safeguard against potential flaws or discrepancies that may have gone undetected by the agents themselves. This reduces the likelihood of biases, blind spots, or unforeseen edge cases that only a human observer can identify.

4. FUTURE DIRECTIONS

We view this paper as a foundational and pragmatic effort to harness the power of agentic systems for tasks relevant to the financial services industry. Looking ahead, research in this area should focus on self-improving agents, a proponent of self-learning, where agents enhance their initial prompts and adapt to roles that weren't initially assigned to them. A good example would be an adaptive learning agent that continuously improve its performance through the interactions it had in the past and the various feedbacks it got. Another area worthy of in-depth investigation is the research and development of crew-generating agentic systems. This could lead to more agile and responsive systems - for example, a crew presented with a prompt to generate its own agents, tools, and tasks required for specific operations such as modeling or model risk management.

ACKNOWLEDGEMENT

We would like to thank Sharon O'Shea Greenbach (Sr. Counsel & Director, Regulatory Policy at DFS) for her constructive comments relevant to compliance challenges that emerge within the financial services sector and for carefully reviewing the manuscript. Ashkan Golgoon benefited from stimulating discussions with Amirhossein Tajdini and Khashayar Filom. The opinions expressed herein are solely our own and do not reflect the views or opinions of our employer. The authors have not used any customer data or internal data from Discover Financial Services for their experiments.

REFERENCES

- [1] A. Abid, M. Farooqi, and J. Zou. Persistent anti-muslim bias in large language models. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, pages 298–306, 2021.
- [2] S. G. Ayyamperumal and L. Ge. Current state of llm risks and ai guardrails. *arXiv preprint arXiv:2406.12934*, 2024.
- [3] S. Bahoo, M. Cucculelli, X. Goga, and J. Mondolo. Artificial intelligence in finance: a comprehensive review through bibliometric and content analysis. *SN Business & Economics*, 4(2):23, 2024.
- [4] M. Besta, N. Blach, A. Kubicek, R. Gerstenberger, M. Podstawski, L. Gianinazzi, J. Gajda, T. Lehmann, H. Niewiadomski, P. Nyczyk, et al. Graph of thoughts: Solving elaborate problems with large language models. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, pages 17682–17690, 2024.
- [5] A. Chan, R. Salganik, A. Markelius, C. Pang, N. Rajkumar, D. Krashennikov, L. Langosco, Z. He, Y. Duan, M. Carroll, et al. Harms from increasingly agentic algorithmic systems. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pages 651–666, 2023.
- [6] C.-M. Chan, W. Chen, Y. Su, J. Yu, W. Xue, S. Zhang, J. Fu, and Z. Liu. Chateval: Towards better llm-based evaluators through multi-agent debate. *arXiv preprint arXiv:2308.07201*, 2023.
- [7] G. Chen, L. Fan, Z. Gong, N. Xie, Z. Li, Z. Liu, C. Li, Q. Qu, S. Ni, and M. Yang. Agentcourt: Simulating court with adversarial evolvable lawyer agents. *arXiv preprint arXiv:2408.08089*, 2024.
- [8] W. Chen, Y. Su, J. Zuo, C. Yang, C. Yuan, C. Qian, C.-M. Chan, Y. Qin, Y. Lu, R. Xie, et al. Agentverse: Facilitating multi-agent collaboration and exploring emergent behaviors in agents. *arXiv preprint arXiv:2308.10848*, 2023.
- [9] Y. Cheng, C. Zhang, Z. Zhang, X. Meng, S. Hong, W. Li, Z. Wang, Z. Wang, F. Yin, J. Zhao, et al. Exploring large language model based intelligent agents: Definitions, methods, and prospects. *arXiv preprint arXiv:2401.03428*, 2024.
- [10] CrewAI. Multi AI agent systems with crewAI - deeplearning.ai, 2024. [Online; accessed 12. Aug. 2024].
- [11] crewAIInc. crewAI: Cutting-edge framework for orchestrating role-playing, autonomous AI agents. <https://github.com/crewAIInc/crewAI/>, 2024.
- [12] Y. Du, S. Li, A. Torralba, J. B. Tenenbaum, and I. Mordatch. Improving factuality and reasoning in language models through multiagent debate. *arXiv preprint arXiv:2305.14325*, 2023.
- [13] S. Han, Q. Zhang, Y. Yao, W. Jin, Z. Xu, and C. He. Llm multi-agent systems: Challenges and open problems. *arXiv preprint arXiv:2402.03578*, 2024.
- [14] J. He, C. Treude, and D. Lo. Llm-based multi-agent systems for software engineering: Vision and the road ahead. *arXiv preprint arXiv:2404.04834*, 2024.

- [15] J. J. Horton. Large language models as simulated economic agents: What can we learn from homo silicus? Technical report, National Bureau of Economic Research, 2023.
- [16] W. Hua, X. Yang, Z. Li, C. Wei, and Y. Zhang. Trustagent: Towards safe and trustworthy llm-based agents through agent constitution. *arXiv preprint arXiv:2402.01586*, 2024.
- [17] D. Huang, Q. Bu, J. M. Zhang, M. Luck, and H. Cui. Agentcoder: Multi-agent-based code generation with iterative testing and optimisation. *arXiv preprint arXiv:2312.13010*, 2023.
- [18] Y. Huang, C. Zhou, K. Cui, and X. Lu. A multi-agent reinforcement learning framework for optimizing financial trading strategies based on timesnet. *Expert Systems with Applications*, 237:121502, 2024.
- [19] H. Jingrong, H. Shan, C. Zhaobin, L. Yu, L. Yingying, et al. Ai-driven digital transformation in banking: A new perspective on operational efficiency and risk management. *Information Systems and Economics*, 5(1):82–90, 2024.
- [20] S. Jinxin, Z. Jiabao, W. Yilei, W. Xingjiao, L. Jiawen, and H. Liang. Cgmi: Configurable general multi-agent interaction framework. *arXiv preprint arXiv:2308.12503*, 2023.
- [21] Kaggle. Credit Card Fraud Detection Dataset. <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud/data>, Mar. 2005. [Online; accessed 3. Oct. 2024].
- [22] Kaggle. Credit Fraud, Dealing with Imbalanced Datasets. <https://www.kaggle.com/code/janiobachmann/credit-fraud-dealing-with-imbalanced-datasets>, Mar. 2005. [Online; accessed 22. Jan. 2025].
- [23] Kaggle. Credit Risk Dataset. <https://www.kaggle.com/datasets/laotse/credit-risk-dataset/data>, 2020. [Online; accessed 3. Oct. 2024].
- [24] Kaggle. Credit Card Approval. <https://www.kaggle.com/datasets/rikdifos/credit-card-approval-prediction>, 2021. [Online; accessed 3. Oct. 2024].
- [25] Kaggle. Credit Card Approval Prediction Using Machine Learning. <https://www.kaggle.com/code/rikdifos/credit-card-approval-prediction-using-ml>, 2021. [Online; accessed 22. Jan. 2025].
- [26] Kaggle. Credit Risk Prediction Training and EDA. <https://www.kaggle.com/code/anshtanwar/credit-risk-prediction-training-and-eda>, 2024. [Online; accessed 22. Jan. 2025].
- [27] V. Kanaparthi. Transformational application of artificial intelligence and machine learning in financial technologies and financial services: A bibliometric review. *arXiv preprint arXiv:2401.15710*, 2024.
- [28] K. J. Koa, Y. Ma, R. Ng, and T.-S. Chua. Learning to generate explainable stock predictions using self-reflective large language models. In *Proceedings of the ACM on Web Conference 2024*, pages 4304–4315, 2024.
- [29] P. Lewis, E. Perez, A. Piktus, F. Petroni, V. Karpukhin, N. Goyal, H. Küttler, M. Lewis, W.-t. Yih, T. Rocktäschel, et al. Retrieval-augmented generation for knowledge-intensive nlp tasks. *Advances in Neural Information Processing Systems*, 33:9459–9474, 2020.
- [30] C. Li, R. Yang, T. Li, M. Bafarassat, K. Sharifi, D. Bergemann, and Z. Yang. Stride: A tool-assisted llm agent framework for strategic and interactive decision-making. *arXiv preprint arXiv:2405.16376*, 2024.
- [31] G. Li, H. Hammoud, H. Itani, D. Khizbullin, and B. Ghanem. Camel: Communicative agents for "mind" exploration of large language model society. *Advances in Neural Information Processing Systems*, 36:51991–52008, 2023.
- [32] N. Li, C. Gao, M. Li, Y. Li, and Q. Liao. Econagent: Large language model-empowered agents for simulating macroeconomic activities. *Preprint*, 2024.
- [33] R. Li, X. Wang, and H. Yu. Exploring llm multi-agents for icd coding. *arXiv preprint arXiv:2406.15363*, 2024.
- [34] Y. Li, Y. Yu, H. Li, Z. Chen, and K. Khashanah. Tradinggpt: Multi-agent system with layered memory and distinct characters for enhanced financial trading performance. *arXiv preprint arXiv:2309.03736*, 2023.
- [35] T. Liang, Z. He, W. Jiao, X. Wang, Y. Wang, R. Wang, Y. Yang, Z. Tu, and S. Shi. Encouraging divergent thinking in large language models through multi-agent debate. *arXiv preprint arXiv:2305.19118*, 2023.
- [36] Y. Ling, X. Jiang, and Y. Kim. Mallm-gan: Multi-agent large language model as generative adversarial network for synthesizing tabular data. *arXiv preprint arXiv:2406.10521*, 2024.
- [37] X. Liu, B. Lan, Z. Hu, Y. Liu, Z. Zhang, W. Zhou, F. Wang, and M. Shieh. Codexgraph: Bridging large language models and code repositories via code graph databases. *arXiv preprint arXiv:2408.03910*, 2024.
- [38] A. Mitra, L. Del Corro, G. Zheng, S. Mahajan, D. Rouhana, A. Cudas, Y. Lu, W.-g. Chen, O. Vrousos, C. Rosset, et al. Agentinstruct: Toward generative teaching with agentic flows. *arXiv preprint arXiv:2407.03502*, 2024.
- [39] N. Mündler, M. N. Müller, J. He, and M. Vechev. Code agents are state of the art software testers. *arXiv preprint arXiv:2406.12952*, 2024.
- [40] M. Nasr, N. Carlini, J. Hayase, M. Jagielski, A. F. Cooper, D. Ippolito, C. A. Choquette-Choo, E. Wallace, F. Tramèr, and K. Lee. Scalable extraction of training data from (production) language models. *arXiv preprint arXiv:2311.17035*, 2023.
- [41] M. H. Nguyen, T. P. Chau, P. X. Nguyen, and N. D. Bui. Agilecoder: Dynamic collaborative agents for software development based on agile methodology. *arXiv preprint arXiv:2406.11912*, 2024.
- [42] Y. Nie, Y. Kong, X. Dong, J. M. Mulvey, H. V. Poor, Q. Wen, and S. Zohren. A survey of large language models for financial applications: Progress, prospects and challenges. *arXiv preprint arXiv:2406.11903*, 2024.

- [43] H. Pandey, A. Amod, et al. Advancing healthcare automation: Multi-agent systems for medical necessity justification. *arXiv preprint arXiv:2404.17977*, 2024.
- [44] J. S. Park, J. O’Brien, C. J. Cai, M. R. Morris, P. Liang, and M. S. Bernstein. Generative agents: Interactive simulacra of human behavior. In *Proceedings of the 36th annual acm symposium on user interface software and technology*, pages 1–22, 2023.
- [45] T. Park. Enhancing anomaly detection in financial markets with an llm-based multi-agent framework. *arXiv preprint arXiv:2403.19735*, 2024.
- [46] C. Qian, X. Cong, C. Yang, W. Chen, Y. Su, J. Xu, Z. Liu, and M. Sun. Communicative agents for software development. *arXiv preprint arXiv:2307.07924*, 6, 2023.
- [47] Z. Rasheed, M. Waseem, M. Saari, K. Systä, and P. Abrahamsson. Codepori: Large scale model for autonomous software development by using multi-agents. *arXiv preprint arXiv:2402.01411*, 2024.
- [48] S. Schwartz, A. Yaeli, and S. Shlomov. Enhancing trust in llm-based ai automation agents: New considerations and future challenges. *arXiv preprint arXiv:2308.05391*, 2023.
- [49] M. Shamsujjoha, Q. Lu, D. Zhao, and L. Zhu. Towards ai-safety-by-design: A taxonomy of runtime guardrails in foundation model based systems. *arXiv preprint arXiv:2408.02205*, 2024.
- [50] M. Shanahan, K. McDonnell, and L. Reynolds. Role play with large language models. *Nature*, 623(7987):493–498, 2023.
- [51] N. Shinn, F. Cassano, A. Gopinath, K. Narasimhan, and S. Yao. Reflexion: Language agents with verbal reinforcement learning. *Advances in Neural Information Processing Systems*, 36, 2024.
- [52] M. Sudarshan, S. Shih, E. Yee, A. Yang, J. Zou, C. Chen, Q. Zhou, L. Chen, C. Singhal, and G. Shih. Agentic llm workflows for generating patient-friendly medical reports. *arXiv preprint arXiv:2408.01112*, 2024.
- [53] J. Sun, C. Dai, Z. Luo, Y. Chang, and Y. Li. Lawluo: A chinese law firm co-run by llm agents. *arXiv preprint arXiv:2407.16252*, 2024.
- [54] Y. Talebirad and A. Nadiri. Multi-agent collaboration: Harnessing the power of intelligent llm agents. *arXiv preprint arXiv:2306.03314*, 2023.
- [55] D. Tang, Z. Chen, K. Kim, Y. Song, H. Tian, S. Ezzini, Y. Huang, and J. K. T. F. Bissyande. Collaborative agents for software engineering. *arXiv preprint arXiv:2402.02172*, 2024.
- [56] X. Tang, Q. Jin, K. Zhu, T. Yuan, Y. Zhang, W. Zhou, M. Qu, Y. Zhao, J. Tang, Z. Zhang, et al. Prioritizing safeguarding over autonomy: Risks of llm agents for science. *arXiv preprint arXiv:2402.04247*, 2024.
- [57] N. Vadori, L. Ardon, S. Ganesh, T. Spooner, S. Amrouni, J. Vann, M. Xu, Z. Zheng, T. Balch, and M. Veloso. Towards multi-agent reinforcement learning-driven over-the-counter market simulations. *Mathematical Finance*, 34(2):262–347, 2024.
- [58] T. Varshney. NVIDIA Generative AI Technical Blog: Introduction to LLM Agents. <https://developer.nvidia.com/blog/introduction-to-llm-agents/>, 2023.
- [59] X. Wan, H. Deng, K. Zou, and S. Xu. Enhancing the efficiency and accuracy of underlying asset reviews in structured finance: The application of multi-agent framework. *arXiv preprint arXiv:2405.04294*, 2024.
- [60] H. Wang, S. Zhao, Z. Qiang, N. Xi, B. Qin, and T. Liu. Beyond direct diagnosis: Llm-based multi-specialist agent consultation for automatic diagnosis. *arXiv preprint arXiv:2401.16107*, 2024.
- [61] S. Wang, H. Yuan, L. M. Ni, and J. Guo. Quantagent: Seeking holy grail in trading by self-improving large language model. *arXiv preprint arXiv:2402.03755*, 2024.
- [62] S. Wang, H. Yuan, L. Zhou, L. M. Ni, H.-Y. Shum, and J. Guo. Alpha-gpt: Human-ai interactive alpha mining for quantitative investment. *arXiv preprint arXiv:2308.00016*, 2023.
- [63] Z. Wang, D. J. Kim, and T.-H. Chen. Identifying performance-sensitive configurations in software systems through code analysis with llm agents. *arXiv preprint arXiv:2406.12806*, 2024.
- [64] J. Wei, X. Wang, D. Schuurmans, M. Bosma, F. Xia, E. Chi, Q. V. Le, D. Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. *Advances in neural information processing systems*, 35:24824–24837, 2022.
- [65] L. Weidinger, J. Uesato, M. Rauh, C. Griffin, P.-S. Huang, J. Mellor, A. Glaese, M. Cheng, B. Balle, A. Kasirzadeh, et al. Taxonomy of risks posed by language models. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, pages 214–229, 2022.
- [66] M. Wu, Y. Yuan, G. Haffari, and L. Wang. (perhaps) beyond human translation: Harnessing multi-agent collaboration for translating ultra-long literary texts. *arXiv preprint arXiv:2405.11804*, 2024.
- [67] Q. Wu, G. Bansal, J. Zhang, Y. Wu, S. Zhang, E. Zhu, B. Li, L. Jiang, X. Zhang, and C. Wang. Autogen: Enabling next-gen llm applications via multi-agent conversation framework. *arXiv preprint arXiv:2308.08155*, 2023.
- [68] C. Xie, C. Chen, F. Jia, Z. Ye, K. Shu, A. Bibi, Z. Hu, P. Torr, B. Ghanem, and G. Li. Can large language model agents simulate human trust behaviors? *arXiv preprint arXiv:2402.04559*, 2024.
- [69] F. Xing. Designing heterogeneous llm agents for financial sentiment analysis. *arXiv preprint arXiv:2401.05799*, 2024.
- [70] S. Yao, J. Zhao, D. Yu, N. Du, I. Shafran, K. Narasimhan, and Y. Cao. React: Synergizing reasoning and acting in language models. *arXiv preprint arXiv:2210.03629*, 2022.

- [71] Y. Yu, H. Li, Z. Chen, Y. Jiang, Y. Li, D. Zhang, R. Liu, J. W. Suchow, and K. Khashanah. Finmem: A performance-enhanced llm trading agent with layered memory and character design. In *Proceedings of the AAAI Symposium Series*, volume 3, pages 595–597, 2024.
- [72] Y. Yu, Z. Yao, H. Li, Z. Deng, Y. Cao, Z. Chen, J. W. Suchow, R. Liu, Z. Cui, D. Zhang, et al. Fincon: A synthesized llm multi-agent system with conceptual verbal reinforcement for enhanced financial decision making. *arXiv preprint arXiv:2407.06567*, 2024.
- [73] H. Yuan, S. Wang, and J. Guo. Alpha-gpt 2.0: Human-in-the-loop ai for quantitative investment. *arXiv preprint arXiv:2402.09746*, 2024.
- [74] D. Zan, A. Yu, W. Liu, D. Chen, B. Shen, W. Li, Y. Yao, Y. Gong, X. Chen, B. Guan, et al. Codes: Natural language to code repository via multi-layer sketch. *arXiv preprint arXiv:2403.16443*, 2024.
- [75] C. Zhang, X. Liu, M. Jin, Z. Zhang, L. Li, Z. Wang, W. Hua, D. Shu, S. Zhu, X. Jin, et al. When ai meets finance (stock-agent): Large language model-based stock trading in simulated real-world environments. *arXiv preprint arXiv:2407.18957*, 2024.
- [76] J. Zhang, X. Xu, and S. Deng. Exploring collaboration mechanisms for llm agents: A social psychology view. *arXiv preprint arXiv:2310.02124*, 2023.
- [77] W. Zhang, L. Zhao, H. Xia, S. Sun, J. Sun, M. Qin, X. Li, Y. Zhao, Y. Zhao, X. Cai, et al. Finagent: A multimodal foundation agent for financial trading: Tool-augmented, diversified, and generalist. *arXiv preprint arXiv:2402.18485*, 2024.
- [78] Y. Zhang, H. Ruan, Z. Fan, and A. Roychoudhury. Autocoderover: Autonomous program improvement. *arXiv preprint arXiv:2404.05427*, 2024.
- [79] H. Zhao, Z. Liu, Z. Wu, Y. Li, T. Yang, P. Shu, S. Xu, H. Dai, L. Zhao, G. Mai, et al. Revolutionizing finance with llms: An overview of applications and insights. *arXiv preprint arXiv:2401.11641*, 2024.
- [80] Q. Zhao, J. Wang, Y. Zhang, Y. Jin, K. Zhu, H. Chen, and X. Xie. Competeai: Understanding the competition behaviors in large language model-based agents. *arXiv preprint arXiv:2310.17512*, 2023.

APPENDIX A. AGENTIC COLLABORATION IN FINANCIAL MODELING - CREDIT RISK USE CASE

In this section, we present the log derived from running the agentic system on the portfolio credit risk dataset [23]. The entire operation starts with the manager agent initializing the crew with the first request — to conduct an exploratory data analysis. The modeling crew can be viewed as a modeling team in an organization. Each member of the team has specific characteristics. The team also has some tools at its disposal to perform certain functions. The job of the modeling team is to build and evaluate a machine learning model for a particular modeling use case; in this example, we explore the portfolio credit risk. The manager, saddled with the responsibility of managing the end-to-end modeling pipeline, knows the capacity of each team member based on what they have as their expertise. This translates into the manager knowing the tasks to perform and the sequence in which those tasks need to be performed. The manager kicks off the process by delegating the exploratory data analysis to the EDA agent, a Senior Data Scientist. The EDA report after the task is completed shows the shape of the input data: 32,581 rows by 12 columns. The report also contains some other descriptive statistics that are stored in memory and can be retrieved by the manager for use by another agent when the need arises. The next step in the pipeline according to the predefined characteristics given to the manager is feature engineering. Since the information provided by the EDA agent shows that there are some missing values in the data as well as class imbalance, the manager gives the feature engineering agent instructions based on these properties. To avoid data leakage, the train-test split function is applied before the feature engineering step to separate the train and test data. This way the feature engineering agent treats both data with care to make sure there was no contamination. The output from the feature engineering agent shows that class imbalance was handled with SMOTE, and missing values were fixed with KNN imputation. The same style was applied for model selection, where the manager prompts the model selection agent to make a decision using the GridSearchCV method. What we have in this section is a holistic view of how the agentic system tries to execute a modeling workflow using specialized agents.

LOG 3. Portfolio Credit Risk Log

Working Agent: Data Science Manager

Starting Task: Conduct a detailed Exploratory data analysis on the provided dataset located
 ↪ at 'credit/credit_risk_dataset.csv'.

I need to delegate the task of conducting a detailed exploratory data analysis on the
 ↪ provided dataset to the Senior Data Scientist I.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Conduct a detailed exploratory data analysis on the provided dataset located at ',
  ↪ credit/credit_risk_dataset.csv'.",
  "context": "I need a comprehensive report with all relevant insights from the dataset.",
  "coworker": "Senior Data Scientist I"
}
```

I need to use the Exploratory Data Analysis Tool to conduct a detailed analysis on the
 ↪ provided dataset.

Action:

Exploratory Data Analysis Tool

Action Input:

```
{
  "csv_path": "credit/credit_risk_dataset.csv"
}
```

[Data Science Manager] Task output: ## Exploratory Data Analysis Report

Dataset Overview

- The dataset contains 32581 rows and 12 columns.
- The target variable is the 'loan_status' column.
- 2 features have missing values: 'person_emp_length' (2.75%) and 'loan_int_rate' (9.56%).
- The dataset is highly imbalanced with 'loan_status' value 1 at 78.18%.

Feature Analysis

- Numeric Features: 'person_age', 'person_income', 'person_emp_length', 'loan_amnt', 'loan_int_rate', 'loan_percent_income', 'cb_person_cred_hist_length'.
- Categorical Features: 'person_home_ownership', 'loan_intent', 'loan_grade', 'cb_person_default_on_file'.
- Categorical features that need label encoding: 'person_home_ownership', 'loan_intent', 'loan_grade', 'cb_person_default_on_file'.
- Positively skewed features: 'person_age', 'person_income', 'person_emp_length', 'loan_amnt', 'loan_int_rate', 'loan_percent_income', 'cb_person_cred_hist_length'.

Descriptive Statistics

- 'person_age': Mean=27.73, Std=6.35, Min=20.0, Max=144.0
- 'person_income': Mean=66074.85, Std=61983.12, Min=4000.0, Max=6000000.0

```
- 'person_emp_length': Mean=4.79, Std=4.14, Min=0.0, Max=123.0
- 'loan_amnt': Mean=9589.37, Std=6322.09, Min=500.0, Max=35000.0
- 'loan_int_rate': Mean=11.01, Std=3.24, Min=5.42, Max=23.22
- 'loan_percent_income': Mean=0.17, Std=0.11, Min=0.0, Max=0.83
- 'cb_person_cred_hist_length': Mean=5.80, Std=4.06, Min=2.0, Max=30.0
```

Correlation Analysis

```
- 'person_age' is highly correlated with 'cb_person_cred_hist_length'.
```

This detailed EDA report provides insights into the dataset and its features, helping in
 ↳ further analysis and modeling.

Working Agent: Data Science Manager

Starting Task: Preprocess the test and train dataset located on 'credit/test.csv' and '
 ↳ credit/train.csv' respectively.

Kindly follow the procedure below and handle the test and train data separately:

- 1) Drop the feature 'person_age' on both the train and test dataset
- 2) Perform label encoding only on the categorical features with fit_transform and
 ↳ transform methods, respectively.
- 3) Use K-Nearest Neighbors (KNN) imputation to fill missing values on the train and test
 ↳ dataset with fit_transform and transform methods, respectively.
- 4) Check the unique values in the target variable named loan_status for the test and train
 ↳ dataset separately to determine if the proportion of any of the classes is equal to
 ↳ or greater than 60%'. if there is class imbalance on any(test or train), perform
 ↳ SMOTE Synthetic Minority Over-sampling Technique(random state = 42) on the test and
 ↳ train dataset separately using fit_resample method.
- 5) Save the new transformed test and train data in the directory 'credit/' as 'test2.csv'
 ↳ and 'train2.csv' respectively.

I need to delegate the task of preprocessing the test and train datasets to the Senior Data
 ↳ Scientist II to ensure that the feature engineering steps are carried out correctly.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Preprocess the test and train datasets according to the specified procedure",
  "context": "I am the Data Science Manager and I need you to preprocess the test and train
    ↳ datasets located on 'credit/test.csv' and 'credit/train.csv' respectively. Follow the
    ↳ provided procedure for feature engineering and handle the test and train data
    ↳ separately. Save the new transformed test and train data in the directory 'credit/'
    ↳ as 'test2.csv' and 'train2.csv' respectively.",
  "coworker": "Senior Data Scientist II"
}
```

I need to carefully follow the provided procedure for feature engineering on the test and
 ↳ train datasets, handle them separately, and save the transformed data in the
 ↳ specified directory.

Action: Python Code Executor Tool

Action Input:

```
{
  "generated_code": "###"
}
```

[Data Science Manager] Task output: ## Feature Engineering Report:

1. Dropping Features:
 - Dropped 'person_age' feature from both the train and test datasets.
2. Label Encoding:
 - Performed label encoding on categorical features using fit_transform and transform methods.
3. K-Nearest Neighbors (KNN) Imputation:
 - Filled missing values on the train and test datasets using KNN imputation with fit_transform and transform methods.
4. Class Imbalance Check and SMOTE:
 - Checked unique values in the target variable 'loan_status' for both test and train datasets.
 - Performed SMOTE (Synthetic Minority Over-sampling Technique) on the train and test datasets separately if any class had a proportion equal to or greater than 60%.
5. Transformed Data Location:
 - Transformed train data saved as 'train2.csv' in the 'credit/' directory.
 - Transformed test data saved as 'test2.csv' in the 'credit/' directory.

Working Agent: Data Science Manager

Starting Task: Select the best machine learning model using the GridSearchCV method on the train dataset located at 'credit/train2.csv'. The target variable is named 'loan_status'. Give the rationale for the selected model.

I need to delegate the task of selecting the best machine learning model using GridSearchCV to the Machine Learning Engineer I, as they are best equipped to handle this task.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Select the best machine learning model using GridSearchCV",
  "context": "The dataset is located at 'credit/train2.csv' and the target variable is named 'loan_status'. The goal is to choose the model that will perform the best on this dataset.",
  "coworker": "Machine Learning Engineer I"
}
```

[Data Science Manager] Task output: ## Model Selection Report

Best Machine Learning Model: XGBOOST

Rationale:

The XGBOOST algorithm was selected as the best machine learning model for the dataset
 ↳ located at 'credit/train2.csv' with the target variable 'loan_status'. This decision
 ↳ was based on the results obtained from the GridSearchCV method, which showed that
 ↳ XGBOOST outperformed other models in terms of accuracy, precision, recall, and F1
 ↳ score.

XGBOOST is known for its high performance and efficiency in handling complex datasets,
 ↳ making it a suitable choice for this credit risk modeling project. Additionally,
 ↳ XGBOOST is capable of handling class imbalances effectively, which is crucial in
 ↳ credit risk modeling where the target variable may have an uneven distribution.

Overall, the XGBOOST algorithm was deemed the most appropriate model for this dataset based
 ↳ on its superior performance metrics and ability to handle the specific challenges
 ↳ posed by credit risk modeling tasks.

Working Agent: Data Science Manager

Starting Task: Tune the hyperparameters of the selected model. Use only 5% of the train
 ↳ dataset for faster outputs. The random state and/or seed should be set to 42.

Save the result as a txt file with the name 'hyper_params.txt' in the directory 'credit/'.

I need to delegate the task of tuning the hyperparameters of the XGBoost model to the Senior
 ↳ Machine Learning Engineer I using only 5% of the dataset located at 'credit/train2.
 ↳ csv'.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Tune hyperparameters of XGBoost model",
  "context": "Use 5% of the dataset located at 'credit/train2.csv'. The target feature is
  ↳ named 'loan_status'. Set random state to 42. Use 'n_estimators': [100, 200], '
  ↳ learning_rate': [0.01, 0.1], 'max_depth': [3, 5] for hyperparameter tuning. Save the
  ↳ result as 'hyper_params.txt' in the 'credit/' directory.",
  "coworker": "Senior Machine Learning Engineer I"
}
```

I need to generate and execute Python code to tune the hyperparameters of the XGBoost model
 ↳ using 5% of the dataset, with specific parameters and values provided. I must save
 ↳ the result as 'hyper_params.txt' in the 'credit/' directory.

Action: Python Code Executor Tool

Action Input: {'generated_code': '###'}

[Data Science Manager] Task output: ## Hyperparameter Tuning Report

Best Hyperparameters for XGBoost Model

- Learning Rate: 0.1
- Max Depth: 5
- Number of Estimators: 200

These hyperparameters were tuned using 5% of the dataset located at 'credit/train2.csv' with
 ↳ the target feature 'loan_status' and a random state of 42. The results were saved in
 ↳ the 'hyper_params.txt' file in the 'credit/' directory.

Working Agent: Data Science Manager

Starting Task: Train the selected model from the model selection agent.

Data:

- Use the train data provided dataset located at 'credit/train2.csv'.

Training:

- Train the selected machine learning model using the train dataset and the best
 ↳ hyperparameters.

Saving:

- Save the trained model in the directory 'credit/' as 'model.joblib'.

I need to delegate the task of training the selected machine learning model to the Senior
 ↳ Machine Learning Engineer II.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Train the selected machine learning model using the train dataset and the best
  ↳ hyperparameters.",
  "context": "The best hyperparameters for the XGBoost model are: Learning Rate: 0.1, Max
  ↳ Depth: 5, Number of Estimators: 200. These were tuned using 5% of the dataset located
  ↳ at 'credit/train2.csv' with the target feature 'loan_status' and a random state of
  ↳ 42. The results were saved in the 'hyper_params.txt' file in the 'credit/' directory
  ↳ .",
  "coworker": "Senior Machine Learning Engineer II"
}
```

I need to generate and execute a Python code to train the selected XGBoost model using the
 ↳ best hyperparameters provided by the model selection agent.

Action:

Python Code Executor Tool

Action Input:

```
{
  "generated_code": "###"
}
```

[Data Science Manager] Task output: ## Model Training Report

Training Conclusion

The training of the selected XGBoost model was successfully completed using the best
 ↳ hyperparameters obtained through tuning. The model was trained on the train dataset
 ↳ located at 'credit/train2.csv' with the target variable 'loan_status'.

Location of the Saved Model

The trained XGBoost model has been saved at 'credit/model.joblib'.

Thank you for the opportunity to complete this task successfully.

Working Agent: Data Science Manager

Starting Task: Evaluate the performance of the trained model located at 'credit/model.joblib'

↪ ' The test data for this evaluation is located at 'credit/test2.csv'. The result
↪ should contain all the performance metrics accuracy, F1-score, recall, precision, and
↪ auc.

I need to delegate the task of evaluating the model to the Senior Machine Learning Engineer

↪ III and provide all the necessary context for them to execute the task successfully.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Evaluate the performance of the model located at 'credit/model.joblib' using the
  ↪ test data located at 'credit/test2.csv'. Create a dict variable called 'result'
  ↪ containing accuracy, F1-score, recall, precision, top capture rate, and auc.",
  "context": "The model evaluation is crucial for assessing the effectiveness of the credit
  ↪ risk modeling project. The target variable is 'loan_status'. The evaluation metrics
  ↪ needed are accuracy, F1-score, recall, precision, and auc. The model file is 'credit/
  ↪ model.joblib' and the test data is 'credit/test2.csv'.",
  "coworker": "Senior Machine Learning Engineer III"
}
```

I need to generate and execute Python code to evaluate the performance of the model located

↪ at 'credit/model.joblib' using the test data located at 'credit/test2.csv'. I should
↪ create a dict variable called 'result' containing accuracy, F1-score, recall,
↪ precision, top capture rate, and auc. Finally, I need to print the result variable.

Action:

Python Code Executor Tool

Action Input:

```
{
  "generated_code": "###"
}
```

[Data Science Manager] Task output: Model Evaluation Metrics:

```
- Accuracy: 0.9536671924290221
- F1-score: 0.951844262295082
- Recall: 0.9158123028391167
- Precision: 0.9908276450511946
- AUC: 0.9536671924290221
```


The evaluation of the model located at 'credit/model.joblib' using the test data from 'credit/test2.csv' has been successfully completed. The performance metrics have been calculated and displayed above. This information is crucial for assessing the effectiveness of the credit risk modeling project.

APPENDIX B. FRAUD DETECTION DATASET EXPERIMENT - SMOTE UPSAMPLING

This section presents the results obtained by employing the SMOTE upsampling method to enhance the representation of fraudulent instances through feature engineering. Figure 10 shows a graphical representation of the evaluation metrics on the test data. The results indicate an accuracy of 97.28%, an F1-score of 97.21%, precision at 99.82%, recall reaching 94.72%, and an AUC value of 97.28%. The model risk management analysis shows slight decline in performance for shifted inputs. The accuracy declined from 97.28% to 93.19%, F1-score from 97.21% to 92.69%, and AUC from 97.28% to 93.19%. This indicates that the model, although it had excellent metrics on the test dataset, had a slight decline during stress testing. The model was able to maintain its original performance, with the accuracy, F1-score, and AUC remaining at approximately 97%. This suggests that the model is capable of handling outliers in the data and is not overly sensitive to the presence of anomalous instances.

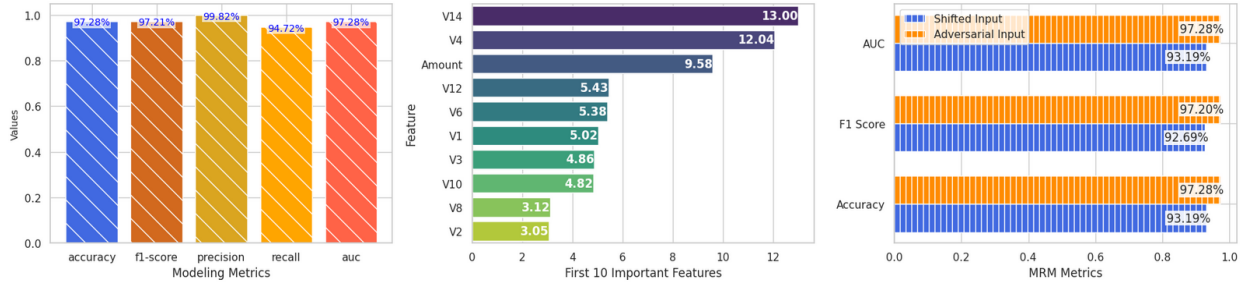


FIGURE 10. Performance report for oversampling the fraud detection dataset

APPENDIX C. AGENTS COLLABORATION - MODEL RISK MANAGEMENT FOR PORTFOLIO CREDIT RISK

The Model Risk Management (MRM) crew plays a crucial role in this research. We briefly discuss the various interactions among agents for the credit-risk use case (refer to Log 4). The manager's responsibility is to ensure that the model trained by the modeling team is compliant. This is achieved by verifying the steps taken by the modeling team to produce a result and assessing the model's performance benchmarks in relation to business objectives. To kick off the process, the manager delegates the documentation compliance task to the "Documentation Compliance Checker Agent," with the role "Senior Data Scientist." This compliance checker utilizes a RAG tool to validate each component of the modeling procedure against the organizational modeling guide. As demonstrated in Log 4, the first prompt was to review the modeling documentation and the modeling guide provided by the organization. This establishes a foundation for the agent to ensure that the modeling team adhered to the organization's modeling procedures. The output of this agent is stored in memory and can be used subsequently as context for other agents performing similar tasks. The "Model Replication Agent" is responsible for independently training and evaluating the selected model in a separate environment using the hyperparameters provided by the modeling crew. This ensures that the model can be reliably reproduced under the same conditions. The agent's primary objective is to validate the model's

replicability and assess its performance benchmarks, identifying any discrepancies that may arise. This helps ensure consistency, robustness, and reliability in the model's behavior across different environments. The "Conceptual Soundness Agent" comes into play when the manager requests validation regarding the model's alignment with business assumptions, performance metrics, and interpretability. With this information, the manager can request for additional tasks to be performed, as detailed in the log; such as testing the trained model under extreme scenarios. This task is assigned to the "Outcome Analyzer Agent", responsible for perturbing the original data to generate adversarial and shifted inputs.

LOG 4. Model Risk Management - Log

Working Agent: Manager - Model Risk Management

Starting Task: Check the modeling documentation result with the organizational modeling

- ↪ guide/blueprint to verify if the modeling procedure conforms with the organizational
- ↪ modeling blueprint. The path to the PDF file containing the organizational modeling
- ↪ guide is 'credit/modeling_blueprint.pdf'. The path to the txt file containing the
- ↪ modeling team's documention file is 'credit/crew_documentation.txt'.

I need to delegate the task of checking the modeling documentation result with the

- ↪ organizational modeling guide to the Senior Data Scientist - Documentation Compliance
- ↪ Check.

Action: Delegate work to coworker

Action Input:

```
{
  "task": "Check the modeling documentation result with the organizational modeling guide/
  ↪ blueprint to verify if the modeling procedure conforms with the organizational
  ↪ modeling blueprint.",
  "context": "The path to the PDF file containing the organizational modeling guide is '
  ↪ credit/modeling_blueprint.pdf'. The path to the txt file containing the modeling team
  ↪ 's documention file is 'credit/crew_documentation.txt'.",
  "coworker": "Senior Data Scientist - Documentation Compliance Check"
}
```

I need to use the Retrieval Augmented Generation(RAG) Tool to compare the modeling team's

- ↪ documentation with the organizational modeling guide.

Action:

Retrieval Augmented Generation(RAG) Tool

Action Input:

```
{
  "pdf_path": "credit/modeling_blueprint.pdf",
  "model_doc_path": "credit/crew_documentation.txt"
}
```

Reading modeling documentation from the modeling crew....

Modeling Documentation

Exploratory Data Analysis

- The dataset contains 32581 rows and 12 columns.
- The target variable is the loan_status column.
- 2 features have missing values.....truncated

Reading the modeling guide....

Comprehensive Guide to Machine Learning Pipeline Development

Introduction:

Machine learning pipeline development is a structured process that involves a series of stages to build and deploy machine learning models effectively. In this document, we will

- ↪ provide a detailed overview of each stage in the machine learning pipeline,
- ↪ including Exploratory Data Analysis (EDA), Feature Engineering, Model Selection,
- ↪ Hyperparameter Tuning, Model Training, and Model Evaluation....truncated

[Manager - Model Risk Management] Task output: The modeling documentation provided by the

- ↪ modeling team aligns well with the processes described in the organizational modeling
- ↪ guide. The team followed a structured approach starting from Exploratory Data
- ↪ Analysis (EDA), Feature Engineering, Model Selection, Hyperparameter Tuning, Model
- ↪ Training, and Model Evaluation, which are all key stages outlined in the
- ↪ organizational modeling guide. The documentation showcases a thorough understanding
- ↪ of the dataset, handling missing values, encoding categorical features, addressing
- ↪ class imbalances, model selection, hyperparameter tuning, and model evaluation, which
- ↪ are in line with the best practices recommended in the organizational modeling guide
- ↪ . Overall, the modeling team's documentation demonstrates a comprehensive and well-
- ↪ structured approach to machine learning pipeline development, reflecting a high level
- ↪ of adherence to the organizational modeling blueprint.

Working Agent: Manager - Model Risk Management

Starting Task: Train and evaluate a machine learning model, then compare its metrics with

- ↪ that of the modeling team's metrics to see if they are the same. The train and test
- ↪ data can be found in 'credit/train2.csv' and 'credit/test2.csv' respectively.

The selected Model is - {'XGB00ST'}.

The hyperparameters used are {'learning_rate': 0.1, 'max_depth': 5, 'n_estimators': 200}.

Train the model with the train data and hyperparameters above and evaluate it using test

- ↪ data. Compare its accuracy, F1-score, recall, precision, and auc, with the metrics
- ↪ from the modeling team.

Modeling teams metrics:

- Accuracy: 0.9536671924290221
- F1-score: 0.951844262295082
- Recall: 0.9158123028391167
- Precision: 0.9908276450511946
- AUC: 0.9536671924290221

The target feature is named 'loan_status'.

I need to replicate the modeling team's machine learning model and compare its metrics with

- ↪ the team's metrics to determine if the model is replicable. I should start by
- ↪ training and evaluating the model using the provided train and test data, as well as
- ↪ the specified hyperparameters for the XGBoost model.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Model replication",
```

```

"context": "Train and evaluate the XGBoost model using the provided train and test data,
↳ as well as the specified hyperparameters. Compare the model's metrics (accuracy, F1-
↳ score, recall, precision, AUC) with the modeling team's metrics to determine if the
↳ model is replicable.",
"coworker": "Senior Machine Learning Engineer - Model Replication",
"kwargs": {
  "model_name": "XGBoost",
  "hyperparameters": {
    "learning_rate": 0.1,
    "max_depth": 5,
    "n_estimators": 200
  },
  "train_data_path": "credit/train2.csv",
  "test_data_path": "credit/test2.csv",
  "target_feature": "loan_status",
  "modeling_team_metrics": {
    "accuracy": 0.9536671924290221,
    "f1_score": 0.951844262295082,
    "recall": 0.9158123028391167,
    "precision": 0.9908276450511946,
    "auc": 0.9536671924290221
  }
}
}

```

I need to generate and execute Python code to train and evaluate the XGBoost model with the
 ↳ given hyperparameters and compare its metrics with the modeling team's metrics to see
 ↳ if they match.

Action: Python Code Executor Tool

Action Input: {"generated_code": "###"}

[Manager - Model Risk Management] Task output: Model Replication Report:

The XGBoost model was successfully replicated using the provided train and test data, along
 ↳ with the specified hyperparameters. The model's evaluation metrics were compared with
 ↳ the modeling team's metrics to determine replicability.

Model Evaluation Metrics:

- Accuracy: 0.9536671924290221
- F1-score: 0.951844262295082
- Recall: 0.9158123028391167
- Precision: 0.9908276450511946
- AUC: 0.9536671924290221

Result:

```

{
  "Accuracy": 0.9536671924290221,
  "F1-score": 0.951844262295082,
  "Recall": 0.9158123028391167,
  "Precision": 0.9908276450511946,
  "AUC": 0.9536671924290221
}

```

```
}

```

The model was successfully replicated, and the metrics align with the modeling team's
 ↳ metrics, indicating a high level of replicability in the model development process.

Working Agent: Manager - Model Risk Management

Starting Task: Show the feature importance and explainability of the trained model located
 ↳ at 'credit/model.joblib'. Print out the first 10 features that contributed to the
 ↳ results using the test data.

When feature importance is established, give the rationale and reason for this process.
 ↳ Based on the feature importance write a narrative that confirms or refutes model
 ↳ compliance to standard practice. The test data can be found in 'credit/test2.csv'.
 ↳ The target feature is named, 'loan_status'.

I need to delegate the task of showing feature importance and explainability of the trained
 ↳ model to the Senior Model Validation Analyst - Conceptual Soundness.

Action: Delegate work to coworker

Action Input:

```
{
  "task": "Show feature importance and explainability of the trained model",
  "context": "The trained model is located at 'credit/model.joblib'. Show the first 10
    ↳ features that contributed to the results using the test data located in 'credit/test2
    ↳ .csv'. If the model is Logistic Regression or Support Vector Machine, use coef_
    ↳ attribute of the fitted model to obtain the feature importances. If its Decision Tree
    ↳ , Random Forest, XGBoost, Gradient Boosting, or CatBoost, use the
    ↳ feature_importances_ attribute of the fitted model to obtain the feature importances.
    ↳ If the model is Naive Bayes, use the feature_log_prob_ attribute of the fitted model
    ↳ to obtain the feature importances. The higher the log probability, the more
    ↳ important the feature.",
  "coworker": "Senior Model Validation Analyst - Conceptual Soundness"
}
```

I need to generate and execute Python code to show the feature importance and explainability
 ↳ of the trained model using the test data provided. I must consider the type of model
 ↳ and use the appropriate attribute to obtain the feature importances.

Action: Python Code Executor Tool

Action Input: {"generated_code": "###"}

[Manager - Model Risk Management] Task output: {

```
  "top_10_features": {
    "loan_grade": 0.297810,
    "loan_percent_income": 0.222958,
    "cb_person_default_on_file": 0.216813,
    "person_home_ownership": 0.116931,
    "loan_intent": 0.062550,
    "person_income": 0.041828,
    "person_emp_length": 0.018830,
    "cb_person_cred_hist_length": 0.009336,
    "loan_int_rate": 0.006756,
    "loan_amnt": 0.006189
```

```
}
}
```

Based on the feature importance analysis, the top 10 features that contributed to the
 ↳ results are listed above. The feature importance values indicate the relative
 ↳ importance of each feature in predicting the target variable 'loan_status'.

The model appears to be compliant with standard practice as it considers relevant features
 ↳ such as loan grade, loan percent income, default history, home ownership, loan intent
 ↳ , income, employment length, credit history length, interest rate, and loan amount.
 ↳ These features align with common factors that are typically considered in loan
 ↳ approval processes, indicating that the model is capturing important aspects of the
 ↳ decision-making process.

Working Agent: Manager - Model Risk Management

Starting Task: Conduct additional testing on the model located at 'credit/model.joblib'. The
 ↳ test data can be found in 'credit/test2.csv'. The target feature is 'loan_status'.
 To conduct this additional testing you need to perturb the test data to simulate extreme or
 ↳ hypothetical scenarios, such as:

1. Shifted inputs - significant shifts in input data distributions.
 Exclude the categorical variables from this process.
2. Outlier and adversarial inputs. Example: 'X_test_outliers = X_test.copy()
 X_test_outliers.loc[0] = X_test_outliers.loc[0] + 1000'

Evaluate the model's robustness and stability on the shifted inputs and on the adversarial/
 ↳ outlier inputs using performance benchmarks like accuracy, F1-score, precision, AUC,
 ↳ etc.

I need to delegate the task of conducting additional testing of the model to the Outcome
 ↳ Analyzer agent to evaluate the model's robustness under extreme scenarios.

Action:

Delegate work to coworker

Action Input:

```
{
  "task": "Evaluate the model's robustness under extreme scenarios by conducting additional
  ↳ testing.",
  "context": "I need you to evaluate the model's performance on shifted inputs and
  ↳ adversarial/outlier inputs using performance benchmarks like accuracy, F1-score,
  ↳ precision, AUC, etc. The test data is located at 'credit/test2.csv', and the model is
  ↳ located at 'credit/model.joblib'. Please perturb the test data to simulate extreme
  ↳ scenarios as described in the task description.",
  "coworker": "Senior Model Validation Analyst - Outcome Analyzer"
}
```

I need to generate and execute Python code to test the model's robustness under extreme
 ↳ scenarios as described in the task description. I will need to perturb the test data
 ↳ to simulate shifted inputs and adversarial/outlier inputs, then evaluate the model's
 ↳ performance using various performance benchmarks.

Action: Python Code Executor Tool

Action Input:

```
{
  "generated_code": "###"
}
```

[Manager - Model Risk Management] Task output: {

```
  "outcome_analysis_report": "The outcome analysis report indicates that the model's
    ↳ performance under extreme scenarios was evaluated. The model demonstrated a higher
    ↳ level of robustness and stability when tested on adversarial/outlier inputs compared
    ↳ to shifted inputs. The accuracy, F1 score, precision, and ROC AUC metrics were
    ↳ significantly better for adversarial/outlier inputs, suggesting that the model is
    ↳ more reliable in handling extreme scenarios that deviate from the normal data
    ↳ distribution.",
  "result": {
    "shifted_inputs": {
      "accuracy": 0.862,
      "F1_score": 0.869,
      "precision": 0.828,
      "ROC_AUC": 0.862
    },
    "adversarial_outlier_inputs": {
      "accuracy": 0.954,
      "F1_score": 0.952,
      "precision": 0.991,
      "ROC_AUC": 0.954
    }
  }
}
```