

Team Members:

Logan Pasternak: lp586

Minsky Luo: ml2055

Pranav Angiya Janarthanan: pa446

Project Report 1 (Group 3)

System Functionalities:

This section of our team's report provides a comprehensive overview of the core functionalities of our stock trading application, which users will be able to engage with upon the release of the final build. Section I outlines the authentication mechanisms that ensure secure user access. Section II details the process of executing share transactions within the platform. Section III explores portfolio management features designed to enhance user experience. Section IV examines the structure and usability of our browser-based user interface. Section V goes over methods of account management. Finally, Section VI describes the implementation of our AI-powered chat agent and its role in assisting users. Through this structured analysis, we aim to present a clear understanding of our application's key components and functionalities.

I. Login Authentication

Our authentication system will feature three primary functionalities: user account creation, account login, and account recovery.

Account Creation

The account creation process requires users to complete a form containing the following fields: username, email, password, risk tolerance, investment experience, and investment goals. Figure 1 illustrates the user interface layout for this process.

Figure 1: Account Creation Screens

The username and password serve as the primary credentials for logging into an account. To enhance security, all submitted passwords are encrypted using the bcrypt library before being stored in our SQL database. This encryption ensures the protection of user credentials against unauthorized access.

Once a user's identity is verified, all subsequent interactions with our brokerage platform are secured using JSON Web Tokens (JWTs), implemented via the jsonwebtoken library. These tokens expire after two hours or upon user logout, providing an additional layer of security against unauthorized access and cyber threats.

Account Recovery

A user's email serves as the primary method for account recovery in cases where they have forgotten their username or password. Upon request, a recovery code is sent to the user via email using the nodemailer module. The user can then enter this code on an account recovery page to reset their credentials.

AI-Powered Investment Personalization

The risk tolerance, investment experience, and investment goals fields play a crucial role in tailoring our AI-powered financial advisory services. These inputs enable our AI agent to provide investment recommendations aligned with a user's preferences. For example, if a user prefers low-risk investments, the AI agent will prioritize suggestions involving traditionally stable and reputable companies.

II. Share Transaction

There are three fundamental interactions involved in conducting transactions on any brokerage platform: searching for a company's shares, purchasing shares, and selling shares.

Searching for Company Shares

When a client seeks market information on a specific company, they can do so by entering the company's ticker symbol into a search bar. This action triggers a query to a third-party API, retrieving key financial data such as the stock's historical price over the past three days, current share price, trading volume, market capitalization, and other relevant metrics. The details of this data source and extraction process are further discussed in the Source of Data section. The retrieved data will be presented in a structured format, as illustrated in Figure 2, enabling users to assess the stock's performance based on a comprehensive set of indicators. Additionally, within this interface, users will have the option to purchase shares of the searched stock or sell shares they already own.

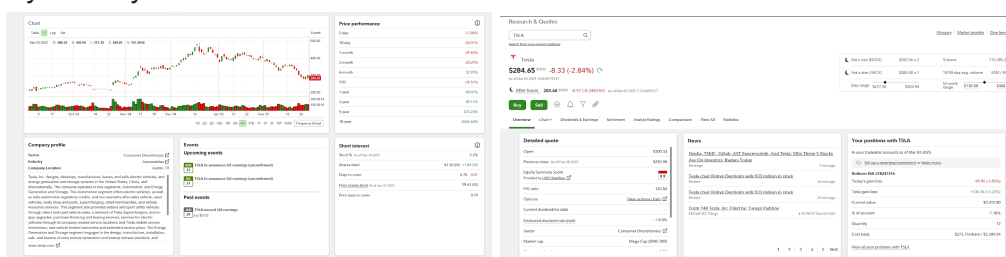


Figure 2: Stock Analysis Page

Buying Shares

The purchasing process is facilitated through an interface similar to the one depicted in Figure 3. The current share price will be prominently displayed, and users will be able to specify the number of shares they wish to acquire. They will also select their preferred payment method, which includes either manual payment or balance-based payment. The manual payment option requires users to complete a form with their credit card details, including the card number, CVV, expiration date, and cardholder name. Upon successfully submitting this information and confirming the transaction, the purchased shares will be automatically added to the user's portfolio.

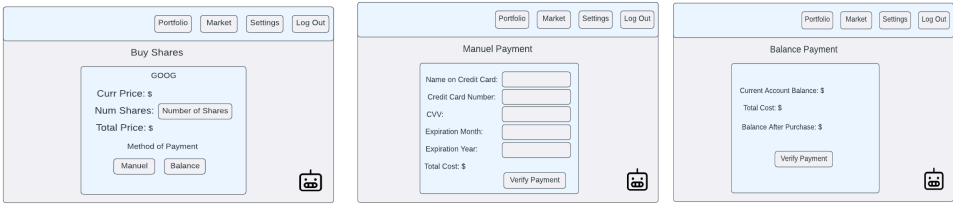


Figure 3: Purchasing Shares

The balance-based payment method leverages funds already deposited in the user’s account, a feature discussed in the Account Management section. Clients can add funds to their account through a manual payment process, which can then be used for future transactions. This eliminates the need to enter credit card details for every purchase, as the required amount will be deducted directly from the user’s available balance.

Selling Shares

The selling process follows a similar structure and is conducted through an interface illustrated in Figure 4. Users can select the number of shares they wish to sell from their existing holdings while viewing the current share price. Upon confirmation of the transaction, the corresponding number of shares will be deducted from their portfolio. If all shares of a particular company are sold, that company will no longer appear in their portfolio. The proceeds from the sale will be credited to the user’s account balance, making them available for future transactions.



Figure 4: Selling Shares

III. Portfolio Management

When first logging onto our brokerage website, the application immediately starts on the portfolio management page. This first page will list all the companies for which one has shares, the current number of shares owned by that individual, the current share price, and a link to the stock’s information page, as discussed in the share transaction section. The overall look of the portfolio management screen will be similar to that displayed in Figure 5.

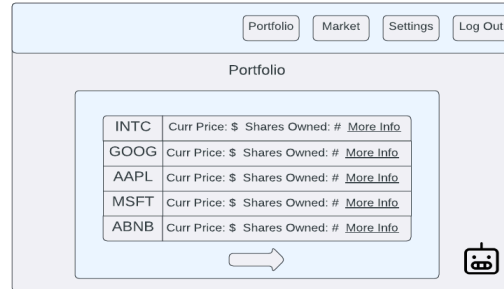


Figure 5: Portfolio Management

IV. Browser User Interface

In the context of our brokerage site, the Browser-Use Interface (BUI) will allow for the automation of complex and time-sensitive tasks involved in financial trading and investment management. The BUI will primarily execute two functions. First, it will be used to automate repetitive actions such as logging into accounts, filling out forms, and executing buy or selling stocks. Second, it will be used to scrape and collect valuable market data from various sources across the web, such as financial news, stock prices, and trends.

V. Account Management

Account management will be facilitated through a dedicated user settings page, as illustrated in Figure 6. This system is designed to enable users to configure and modify their account settings after the initial account creation process. By the conclusion of this project, we aim to implement three core features within the account management system, along with an additional optional enhancement.

The primary functionalities will include the ability for users to update their username and password, modify the model parameters initially set during account creation, and adjust their account balance. Additionally, as a lower-priority objective, we hope to integrate two-factor authentication as an added security measure if time and resources permit.

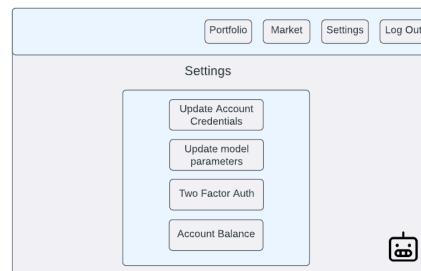


Figure 6: Account Management Page

VI. AI Chat Agent

AI Capabilities

The foundation of our project is an AI-driven chat system designed to provide users with comprehensive stock portfolio insights and investment guidance. This system will have the

capability to deliver personalized feedback on a user's stock portfolio performance, explain common stock trading terms and definitions, and offer tailored investment recommendations based on individual user preferences.

Parameters Utilized by Agent

To achieve these objectives, the AI agent will leverage multiple data sources. Portfolio data, which includes details such as the number of shares held and current share prices, will enable the agent to assess and provide insights into overall portfolio performance. Sentiment-based parameters, established during account creation, will influence the agent's investment recommendations by aligning them with the user's risk tolerance and financial goals. Additionally, user feedback data will be dynamically updated based on interactions, recording responses such as "thumbs up" or "thumbs down" on AI-generated recommendations. This continuous feedback loop will allow the agent to refine its performance over time.

The role of user feedback in enhancing the system's accuracy and adaptability will be explored further in the Testing section of this report, while sample interactions with the AI agent will be presented in the Example Messages section.

Source of Data:

The "Stock Trader with AI Agent" system empowers users with tools to perform various tasks related to stock trading based on their financial agenda. While those agendas are quite subjective and complicated, the system supports them by providing some key functionalities, including the following:

I. User Tasks

- **Stock Research:** Query and analyze historical stock data, trends, and patterns across multiple markets.
- **Trading Strategy:** Receive AI-generated insights for building personalized trade strategies based on market trends, economic forecasts, and user risk appetite.
- **Market Updates:** Access real-time stock prices, financial news, and economic indicators to make informed decisions.
- **Simulated Trading:** Test strategies in a simulated environment using historical data before committing actual trades.

As shown in Figure 2, when the client enters a stock symbol or a common company name in the Research page, the system will find and provide the financial data page of the stock or company that includes a stock price quote (updated every N-minutes), daily open/high/low/volume, price chart (candle-stick), price range, price performance, company profile, company news, event schedule, analysts' ratings, etc. All in one page in a separate tag.

This page is retrieved from the Google Finance site by BUA, the AI agent of the system.

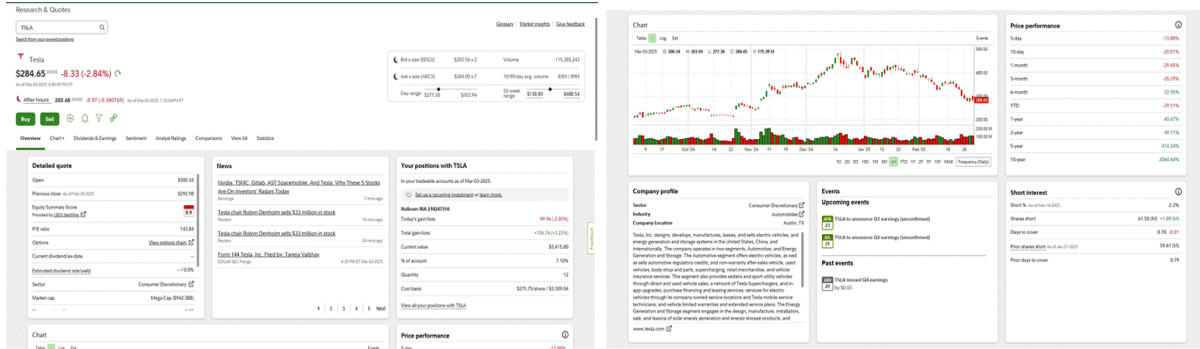


Figure 7: Company Financial Page from Google Finance (provided by BUA)

II. Data Sources

The system gathers public structured data from Yahoo Finance and Google Finance and from the following additional sources:

1. Official company financial reports:

- The official company financial report system mandated by the NYSE is the EDGAR (Electronic Data Gathering, Analysis, and Retrieval) system, which is operated by the U.S. Securities and Exchange Commission (SEC). Publicly traded companies are required to file their financial reports, registration statements, and other disclosures through EDGAR. This system ensures transparency and accessibility for investors and regulators.

2. Historical Stock Market Data:

- APIs like Alpha Vantage, Quandl, and Yahoo Finance for detailed historical performance of stocks.
- Data includes stock prices, volume, market capitalization, and dividend records.

3. Real-Time Stock Prices:

- Use APIs like IEX Cloud, Polygon.io, or Bloomberg for live market prices.
- Provides updates on market fluctuations critical for trading decisions.

4. Economic Indicators:

- Sources like Trading Economics or government-backed platforms (e.g., Federal Reserve Economic Data).
- Includes metrics like GDP, unemployment rate, inflation, interest rates, and others.

5. Financial News and Sentiment:

- News platforms like Google News, Reuters, and AI-powered sentiment analysis tools (e.g., OpenAI for natural language interpretation of financial articles).
- Help users gauge market sentiment.

For unstructured data, websites that BUA accesses to search and sieve for artificial trendy information include, but are not limited to, the following:

[BlackBoxStocks]	A trading chat room with stock and options alerts, along with educational resources.
[InvestorsHub (iHub)]	A forum-based platform where traders discuss stocks, penny stocks, and market trends.
[r/StockMarket]	Stock market discussions, including news, analysis, and general advice.
[r/stocks]	Discussing individual stocks, market trends, and investment strategies.
[r/thinkorswim]	Focused on trading platforms and strategies, with discussions about day trading and swing trading.
[StockTwits]	A social media platform specifically for investors and traders to share ideas, charts, and market insights in real time.
[Stockaholics]	A financial forum covering a wide range of topics, including stock market analysis and trading tips.
[Trade Ideas]	Provides a live trading room for beginners and experienced traders to discuss strategies and market trends.
[TradingView]	Known for its charting tools, it also has a large community where traders share ideas and strategies.

Those community websites are popular sources for discussing the stock market and trading.

These platforms are great for connecting with other traders, learning new strategies, and staying updated on market trends. They are great for engaging with like-minded individuals and staying updated on market trends.

III. The Role of AI Agent

The AI agent (Browser Use) interacts dynamically with these data sources and the user. It:

— **Aggregates Data:** Retrieves and synthesizes information from multiple APIs into coherent insights.

- **Context-Aware Analysis:** Leverages AI endpoints like OpenAI and Gemini to interpret complex data trends and answer nuanced queries.
- **Customization:** Tailors responses based on user profiles (e.g., risk tolerance, preferred sectors).
- **Automation:** Generates AI-assisted trade strategies and summaries that would otherwise require intensive manual research.

IV. Why the AI Agent is Necessary

The complexity and scale of data (historical, real-time, and economic) demand robust AI capabilities for pattern recognition, sentiment analysis, and strategic insights. The AI agent's natural language processing ensures seamless communication with clients and transforms raw data into actionable intelligence. Without the AI agent, user queries would require manual aggregation and analysis, making the process less efficient and more error-prone.

OpenAI GPT-4o and **Gemini 2.0 Flash** are some AI endpoints of a next-generation general-purpose model designed to deliver high-speed, multimodal capabilities for a variety of tasks.

- **Multimodal Abilities:** It can process and generate text, images, and audio, making it versatile for tasks like content creation, document analysis, and more. Outputs text and, in the future, images and audio.
- **Efficiency and Speed:** Optimized for quick responses, it is ideal for users who prioritize speed and simplicity in their AI interactions.
- **Advanced Features:** Includes capabilities like real-time streaming, reasoning, and tool integration, allowing it to handle complex tasks.
- **Use Cases:** Suitable for applications like conversational AI, data analytics, and even video editing, thanks to its extended context window and cost-effective performance.

Browser Use Agent (BUA) is a powerful tool designed to combine browser automation and AI capabilities. It enables embedding browser automation as a part of AI-powered agents, enabling them to interact with web pages dynamically based on context or user input, just what we need for the project.

— Browser Automation

- Automatic browsing tasks like filling out forms, clicking buttons, scrolling, and navigating websites.
- Data Scraping: Extract structured data from web pages without manual intervention.

— AI assisted Automation

- AI Agent interfaces with all major AI chat models such as OpenAI, Google Gemini, or others.
- With a native lightweight model, capable of interpreting user input/queries in natural language, voice, and graphics and executing them intelligently within a web environment.

— Complex Task Handling

Asynchronous multitasking support

— Seamless Integration

- Written in Python and hence it integrates easier to combine with other libraries and APIs to create custom applications.
- Can be programmed to handle a wide range of tasks, from simple navigation to complex workflows like e-commerce order processing or automated reporting.

Message Exchanges:

The client-server communication is designed to ensure smooth interaction between the user and the AI-powered system, especially during a research session.

I. Client Messages

Each message sent from the client to the server has a specific meaning and function:

— Query for Stock Data:

- **Purpose:** Retrieve historical or real-time data for a specific stock or a list of stocks.
- **Parameters:**
 - stock symbol: The ticker symbol(s) of the stock (e.g., "AAPL", "GOOGL").
 - datatype: Specify "historical" or "real-time".
 - time range: Range of dates for historical data.
- **Expected Response:**
 - Historical or current stock performance in JSON format (e.g., prices, volume, trends).

— AI Trade Strategy Request:

- **Purpose:** Generate AI-driven trading strategies based on user-defined criteria.
- **Parameters:**
 - user profile: User-specific information (risk tolerance, sector preferences).
 - strategy type: Specify the type of strategy (e.g., "long-term growth", "momentum trading").

- market conditions: Real-time indicators or trends to consider.
- **Expected Response:**
 - A strategy summary including entry/exit points, recommended stocks, and risk assessment.

— Economic Data Inquiry:

- **Purpose:** Retrieve macroeconomic indicators for analysis.
- **Parameters:**
 - indicator: Type of data required (e.g., "inflation", "GDP").
 - region: Specify the location or country for data (e.g., "US," "Europe").
- **Expected Response:**
 - Economic metrics in JSON format.

— News Sentiment Analysis:

- **Purpose:** Analyze financial news for sentiment and its potential impact.
- **Parameters:**
 - keyword: Topic or company name (e.g., "Tesla", "renewable energy").
 - time range: Date range for articles.
- **Expected Response:**
 - Sentiment scores and summary of news content, highlighting key points.

II. Server Responses

Responses from the server include structured data, typically in JSON format, ensuring easy integration into the user interface. They include:

- Processed stock data or economic indicators.
- AI-generated insights and strategies tailored to the user.
- Summaries of relevant financial news and sentiment analysis.

By designing this structured communication system, users will experience seamless and efficient interactions that maximize the utility of the AI agent in research and trading tasks.

III. An example of a Message Exchange Scenario

Here is a chat scenario example in which the client starts asking, "*Should I buy the dip now?*" This shows how BUA handles the task by responding with questions to clarify, revising the prompts to AI endpoints, and integrating the responses before sending the summary to the client.

1	Client Query: Should I buy the dip now?
---	--

2	<p>BUA Response 1: Clarifying the Context</p> <p>That's a great question! To give you meaningful advice, I'd like to understand your situation a bit better.</p> <ul style="list-style-type: none"> • Are you looking at a specific stock or sector or the market as a whole? • What's your risk tolerance—are you comfortable with high-risk investments, or do you prefer safer options? • Are you considering a short-term trade or a long-term investment strategy?
3	<p>Client Responds:</p> <p>I'm looking at tech stocks, especially companies like Apple (AAPL) and NVIDIA (NVDA). I don't mind taking moderate risks, and this would be for a long-term investment.</p>
4	<p>BUA Response 2: Refining the Query</p> <p>Got it—thank you for sharing! I'll analyze the recent trends for Apple and NVIDIA tech stocks to assess whether this dip might be a good buying opportunity. Additionally, I'll evaluate broader market conditions and sector-specific risks.</p> <p>I may use AI endpoints like OpenAI or Gemini to enhance my research. Here's what I'll do:</p> <ol style="list-style-type: none"> 1. Fetch historical stock price data and recent performance trends for AAPL and NVDA. 2. Evaluate the dip's magnitude compared to past performance (via relevant APIs like Alpha Vantage or Yahoo Finance). 3. Analyze financial news sentiment around the tech sector and these companies. 4. Incorporate market indicators like interest rates, inflation, and broader market volatility. <p>Give me a moment to compile the insights!</p>
5	<p>BUA Processes and Revises Prompts</p> <ul style="list-style-type: none"> • BUA to Historical Data API: <ul style="list-style-type: none"> ◦ Query: "Retrieve historical price trends for AAPL and NVDA over the past year, focusing on recent dips." • BUA to Financial News API: <ul style="list-style-type: none"> ◦ Query: "Analyze recent financial news sentiment related to AAPL, NVDA, and the tech sector. Include major concerns like supply chain disruptions or earnings forecasts." • BUA to Market Indicator API: <ul style="list-style-type: none"> ◦ Query: "Fetch economic data on interest rates and inflation that might impact tech stocks."

6	<p>BUA also integrates AI endpoints:</p> <ul style="list-style-type: none"> • OpenAI Prompt Revision: <ul style="list-style-type: none"> ○ Prompt: "Summarize insights from stock trends and financial news about AAPL and NVDA. Combine this with market data and suggest whether long-term investment during the current dip aligns with a moderate risk appetite."
7	<p>BUA Response 3: Summarizing Findings</p> <p>I've analyzed the current dip and here's what I found:</p> <ol style="list-style-type: none"> 1. Stock Performance: <ul style="list-style-type: none"> ○ AAPL and NVDA have seen dips of 7% and 10%, respectively, over the past two weeks. These dips are moderate compared to their historical corrections (e.g., during earnings seasons), which averaged 5-12%. 2. Financial Sentiment: <ul style="list-style-type: none"> ○ Financial news sentiment is cautiously optimistic. Analysts are highlighting strong fundamentals like cash reserves and robust product pipelines for both companies, though concerns over sector-wide growth amid high interest rates persist. 3. Market Indicators: <ul style="list-style-type: none"> ○ With interest rates steady but inflation slightly elevated, long-term tech investments may experience some volatility. However, tech stocks historically recover well when inflation stabilizes.
8	<p>AI Agent Recommendation:</p> <p>Given your moderate risk tolerance and long-term outlook, the current dip could be a good buying opportunity for AAPL and NVDA, provided you are prepared for potential near-term volatility.</p> <p>Would you like additional insights, or should I help you explore trade strategies further?</p>

This example demonstrates how BUA clarifies the user's intent; revises prompt dynamically, fetches relevant data from APIs, leverages AI endpoint insights, and delivers an integrated response.

As the system grows with more progressive features, much data from the client's portfolio and the database will be automatically incorporated into the prompts that BUA sends to AI endpoints without asking for the clients' inputs. Another essential feature of the system is chat scenario will be guided by predefined templates for BUA to conduct the discussion and to perform the AI tasks.

Infrastructure and Third-Party Tools:

The website is built around a simple web server that contains several main parts. The front end uses simple JavaScript, HTML, and CSS to create an interactive interface. Different pages on the website are dedicated to functions such as account creation, portfolio management, stock research, and trade execution. This setup allows users to move smoothly between checking their investments, researching stocks, and placing trades within a clear and straightforward environment, similar to popular trading platforms like Robinhood, Fidelity, or any other investment websites.

The authentication module is a key part of the system, which handles the sign-up and login processes. This component makes sure that only authorized users can access their accounts. It uses third-party libraries like **Bcrypt** for password hashing and encryption, ensuring that sensitive information remains secure even if the database is compromised. The use of these security measures is vital in protecting user data and meeting the necessary security standards.

On the server side, **Express** is used as the main framework to handle HTTP requests and manage API endpoints. Express simplifies routing and middleware management, making it easier to build a scalable and manageable back end. The framework is useful in organizing the code for trade execution, portfolio management, and other dynamic functionalities, allowing the system to grow as new features are added.

Another important library is **CORS** (Cross-Origin Resource Sharing), which allows the web server to interact securely with APIs hosted on different domains or ports. Using CORS, the system avoids restrictions that could interfere with client-side JavaScript making requests to the server. This is key for ensuring a smooth communication flow between the front end and back end, especially when integrating various services and data sources.

The portfolio management section is designed to give users a clear view of their trading activities and past transactions. It uses a **SQL** database to store and manage data about trades, investment goals, and performance records. SQL is chosen for its ability to handle structured data efficiently, which is essential for running queries on user activity. Additionally, simple charting libraries are used to create visual representations of trading data, making it easier for users to see trends and make informed decisions.

An additional component is the AI chatbot, which acts as a helper when users need market information or advice. The chatbot is built using both front-end JavaScript and back-end integration, which allows live interactions. It relies on third-party APIs provided by OpenAI and BUA to access current market data and interpret user questions. This setup ensures that the chatbot can offer useful, timely responses, assisting users in making more informed trading choices.

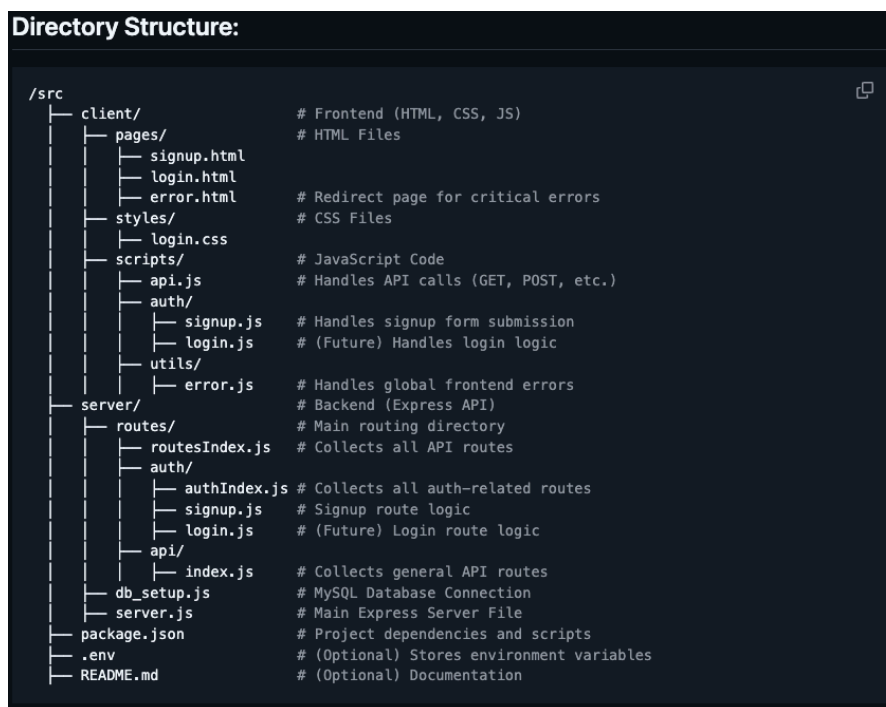


Figure 8: Directory Structure of the Project

The directory structure of the project is organized in a simple and clear way. Files are grouped by their function, such as front-end pages, back-end logic, and database configurations. This grouping makes it easy to add new components or update existing ones without disrupting the overall system. The clear structure aids in quickly finding needed files and helps maintain the project as new features are integrated over time.

Timeline:

The plan of work is organized with milestones that focus on delivering the core trading functionalities first, prioritizing the functionality first, and implementing the key front-end designs once the functionalities are implemented. Since the authentication module is complete, with only its front-end integration remaining, the main focus now is on creating the trading system. This includes the functionality for buying and selling stocks, which will allow the system to start feeding portfolio information into the AI chatbot. The chatbot will use this data to provide insights into users' spending and investing habits, making the trading features critical for the overall user experience.

By early April, before the second presentation, the functionality for trading stocks will be fully implemented. At this stage, users will be able to execute trades on their stock portfolio, and the system will begin to record and display trading activity. Simultaneously, the initial version of the AI chatbot will be integrated, focusing on processing and gathering the stock information as a basis for its responses. This will then further be tailored to include portfolio information to provide more personalized responses.

A detailed timeline of the work plan is as follows:

- **Early April (Before the Presentation):** Trading functionality implementation such as buying and selling stocks.
- **Early April (Around the first presentation):** Integration of the initial AI chatbot to analyze stock. Include components for research on stock and any relevant information.
- **Mid-April:** Further development and fine-tuning of front-end design and AI chatbot utilizing portfolio information.
- **Late April:** Final project completion. All planned features, including research components for stocks and improved front-end design.

This structured approach ensures that the critical trading and chatbot functionalities are delivered early, creating a strong foundation for further development.

System Testing:

System testing for the investment planning system will be conducted at various stages to ensure functionality, security, usability, and performance. All testing will be conducted using Postman.

During the initial backend development phase, testing will verify that the system correctly stores, retrieves, and updates a user's portfolio while ensuring the risk tolerance questionnaire properly captures and retrieves user inputs. The AI query generation will be tested to confirm that only necessary user details and market indicators are included. Additionally, the system's ability to fetch historical and real-time stock data from external APIs will be validated.

As the AI agent is integrated, API query testing will ensure that queries contain all required parameters, and responses from the AI are structured correctly. The system must also handle cases where the AI service is unavailable, slow, or returns incorrect recommendations. Postman will again be utilized for testing these interactions.

Security and privacy testing will focus on data protection and API security. It will be essential to confirm that sensitive user data, such as portfolio details and risk tolerance, is not passed directly to the AI model. Encryption and access control mechanisms will be tested to protect stored data. API authentication testing will be conducted to identify vulnerabilities in API endpoints.