Department of Computer Science & Engineering
The University of Texas at Arlington

Architectural Design Specification
CSE 4316: Senior Design I
Fall 2023

Team Honeycomb
HoneyTrap

Jair Rea
Raed Ali
Hugo Mendoza
Praisy Daniel
Joshua Catalan

Revision History

Revision	Date	Author(s)	Description
0.1	10.01.2015	GH	document creation
0.2	10.05.2015	AT, GH	complete draft
0.3	10.12.2015	AT, GH	release candidate 1
1.0	10.20.2015	AT, GH, CB	official release
1.1	10.31.2015	AL	added design review requests

CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

Our System is comprised of 6 Layers which each has their own sub-systems. First, there's the Profile layer, which holds information about us, like our posts and general details, making sure it's up-to-date. Then comes the Chatbot layer, which pretends to be an elderly person on Facebook, attracting scammers and responding to them. It uses data from our account profile, web scraping tools, and the LLM layer for smart communication. The LLM (Large Language Model) layer connects our chatbot with our language model, ensuring smooth two-way communication. The Communications layer manages interactions between various parts of our chatbot system and the outside world, including API calls, message analysis, and context maintenance. The Web scraping layer identifies vulnerable profiles and potential scammers by assessing various factors. Finally, the Reporting system keeps a record of detected scammers, ensuring we can address potential threats effectively. Together, these components form a robust defense to protect our online personas.

2 System Overview

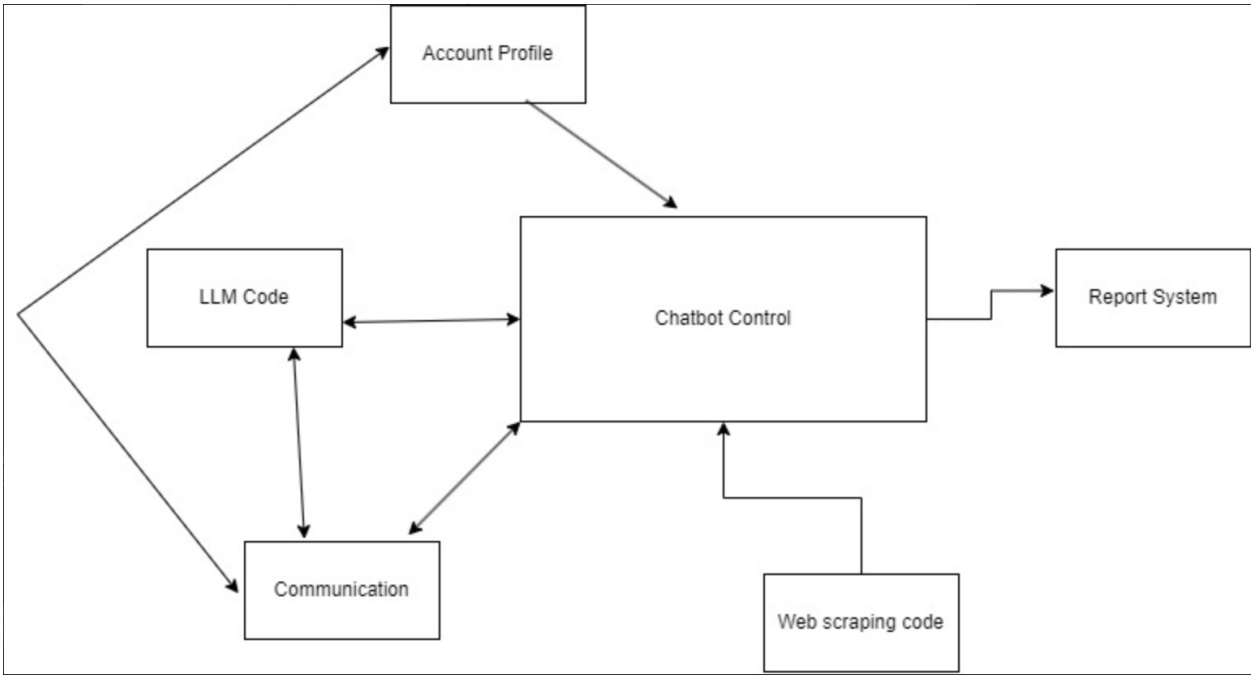

Figure 1: A simple architectural layer diagram

2.1 Layer X Description - Our profile

The Profile layer will have 2 sub systems which are Posts and General Information. The only task of this layer is to essentially store any relevant information pertaining to our persona as we keep updating the account.

2.2 Layer Y Description- Chatbot control/code

The Chatbot layer is composed of 2 sub systems which are Profile connection and Messages. The Chatbotâs task is to connect to the Facebook account of our persona and lure in scammers. Once the scammers have fallen into the honeypot, the Chatbot will begin to reply to the scammers while posing as an elderly person. Replies and messaging will be timed to avoid suspicion. The Chatbot is integrated with a Facebook account through the Account Profile, which provides access to the posts and essential information pertaining to the persona being constructed. A Web scraping layer is employed to furnish the Chatbot with a comprehensive list of potential scammers. The LLM layer plays a crucial role in supplying the Chatbot with the necessary training data. Meanwhile, the communication layer facilitates the exchange of all messages sent and received by the Chatbot. When specific criteria are met, signifying someone as a potential scammer, the system generates a detailed report to address the issue effectively. This multifaceted approach ensures the Chatbot's ability to detect and respond to potential threats in a proactive manner.

2.3 Layer Z Description - LLM code

The LLM layer is composed of 3 subsystems which are the part that connects the bot to the LLM, the part of code that trains our bot using the LLM, and the part of the code that reads what the user says to it and interprets what the user says to the bot. This layer is defined by communicating information to our large language model. The LLM layer will primarily communicate with two other layers, the Chatbot Control

Layer and the Communication Layer. For the Communication Layer, there is a two-way relationship, the messages from the user are from the Communication Layer, and the LLM Code Layer will decode these messages and send an appropriate response to the user which will be sent to the Communication Layer, thus the two-way communication. There are also the API calls that need to be made to connect to our LLM, which would require communication between the Communication Layer. There is also two-way communication with the Chatbot Control Layer since the Chatbot Control is like the central part of the code and it will call the LLM portion of the code(the LLM Layer) and the LLM Layer will tell the Chatbot Control if it detects any suspicious behavior of a scammer and that information will be sent to the Report System Layer from the Chatbot Control Layer.

2.4 Layer A Description - Communications

The communications layer is a crucial component responsible for handling communication between different parts of the chatbot system and external entities. The layer includes features like API calls, messages from interactions with people, and messages the bot sends during the interactions. The communication layer interacts with the LLM code layer to directly get API calls to deliver messages through the bot in real time. The LLM code will feed the incoming message to the communication layer to parse the message, analyze sentiment, and recognize intent from the scammer. Another layer that bidirectionally interacts with the communication layer is the account profile layer which retrieves personal information about the bot pretending to be a real user and provides relevant response that matches with the user's (bot) personal likes and dislikes. The communication layer bidirectionally also interacts with the chatbot control layer to keep track of the current state of the bot and update/manage the context of the messages based on dialogue history that could be found in the chatbot code. We are naming the layers by a variable X,Y,Z,A,B,C, and each of these layers contains multiple subsystems that represent functions or features that come under the respective layer.

2.5 Layer B Description - Reporting Systems

The LLM layer is composed of 2 subsystems which are the Automated Reporting System and the Scammer database. This layer will mostly communicate with the Chatbot Control section. Now the chatbot control section will be told by the LLM Code portion that the current user the bot is speaking to is a scammer and it will send the Chatbot control section the user info and the incriminating chat logs then the Chatbot Control section will parse this information and send this information to the reporting system part of the code. Which will automatically file a report of that user.

2.6 Layer C Description - Web Scraping code

The Web Scraping code will consist of 3 subsystems: vulnerable profile detection, scammer profile detection, list of potential scammers. The web scraping tool will search through facebook profiles and analyze them to identify potentially vulnerable people based on specific criteria such as age as well as specific patterns exhibited on the profile. The tool will also identify potential scammers in a similar manner but will use a different criteria such as posting patterns and keywords which will then be inputted into a file for further analysis to determine the validity of a scammer.

3 SUBSYSTEM DEFINITIONS & DATA FLOW

This section breaks down your layer abstraction to another level of detail. Here you grapically represent the logical subsytems that compose each layer and show the interactions/interfaces between those subsystems. A subsystem can be thought of as a programming unit that implements one of the major functions of the layer. It, therefore, has data elements that serve as source/sinks for other subsystems. The logical data elements that flow between subsystems need to be explicitly defined at this point, beginning with a data flow-like diagram based on the block diagram.

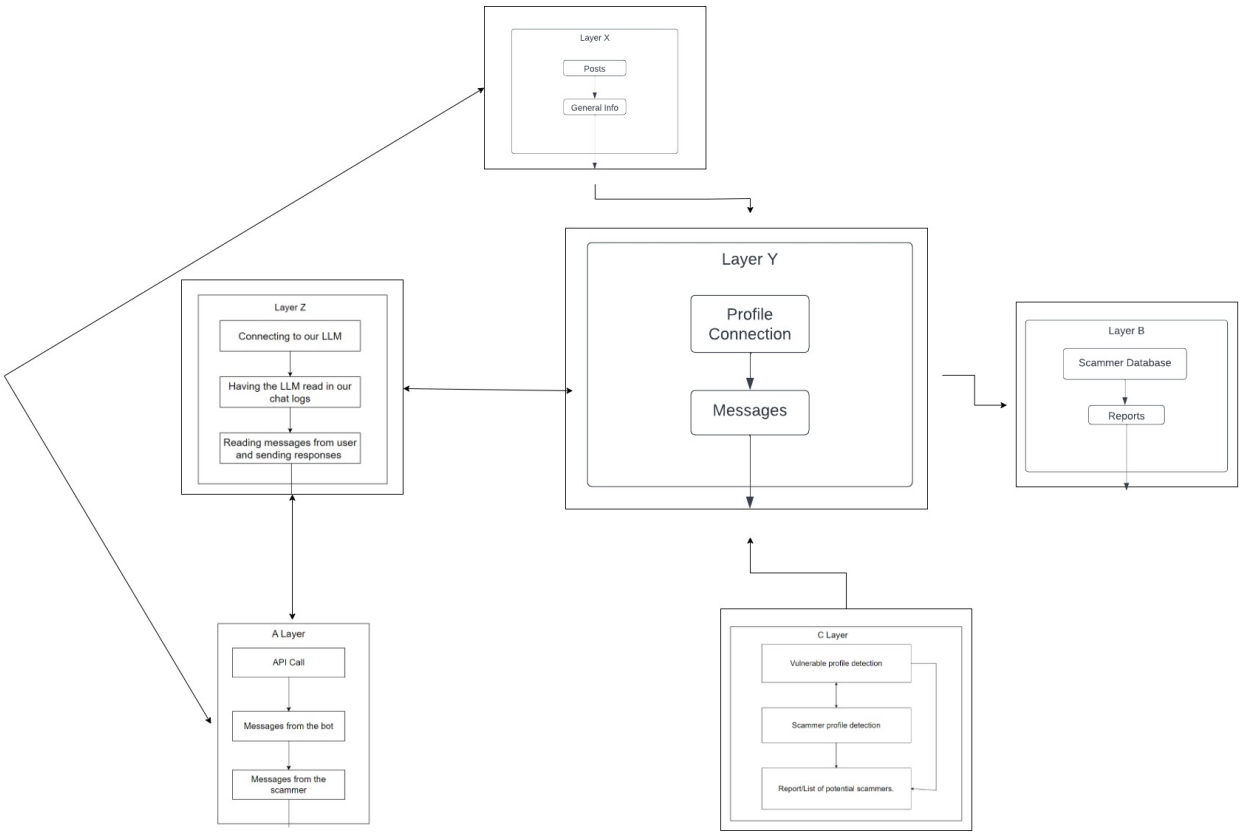

Figure 2: A simple data flow diagram(Please zoom in for a better view)

4 X Layer Subsystems

The Account Profile layer plays a critical role in the fraud detection software project by enabling the creation and management of a Facebook profile, posing as an elderly individual. There are two key systems that are the main focus of the Layer, those being the Team Posts and the General Profile Information. In addition, there is a critical trade-off: Automation vs. Authenticity. As a team, we need to strike the right balance when it comes to messaging as a robotic response will seem suspicious while overly authentic interaction might require extensive resources. Lastly, some special consideration that stem from both subsystems may be: Privacy, Ethical boundaries, Identification, and Security.

4.1 Subsystem 1

This subsystem pertains to the "Team Posts" subsystem. It is a pivotal component within the Account Profile layer of our fraud detection software. Its primary role is to make simulated social interactions. It does this by impersonating an elderly individual. Going more into depth, the subsystem is designed to create and manage posts on the Facebook timeline and engage in conversations with potential scammers. This will gather some general information which will help the LLM learn and adapt.

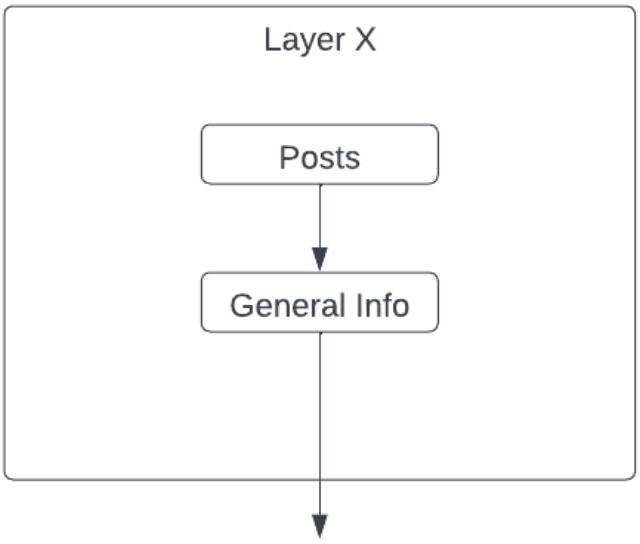

Figure 3: Example subsystem description diagram

4.1.1 Assumptions

Some assumptions to be made are Scalability, User Engagement, and Internet Connectivity. For the first one, we need to assume that our model can efficiently manage a potentially large number of Facebook accounts and interactions simultaneously. It is essential given the volume of interactions required for an effective fraud detection. For the second one, we need to assume that potential scammers will engage in interactions initiated by the subsystem. We need to rely on the assumption that scammers will respond to our posts and comments, providing opportunities for detection. Now for the last assumption, we need to assume that the model will have stable and reliable internet connection for real-time interactions with the platform. Any disruptions may affect the effectiveness of the subsystem.

4.1.2 Responsibilities

The "Team Posts" subsystem in our fraud detection software project has quite a few specific jobs that are really important. First, it's responsible for creating posts that look like they're coming from regular elderly individuals. These posts cover all sorts of topics, like health updates, family events, hobbies, and everyday life stuff, however that's not all it does. It also talks back to people who comment on these posts. And it does so in a way that matches how an elderly person would talk. So, it's all about keeping the conversation real and making sure the responses make sense. Additionally, it keeps an eye on notifications that we get from Facebook. This includes things like comments on posts, friend requests, and direct messages. It responds to these notifications quickly and appropriately, especially when it comes to engaging with potential scammers and other users. Last but not least, it's got to maintain conversations that sound just like real ones. It understands the kind of language and tone elderly people typically use in their conversations. And it adjusts its responses to match the behavior of potential scammers to keep things convincing without making anyone suspicious.

4.1.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labelled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements will pass through this interface.

Table 2: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Profile Creation	Profile picture Profile information	Authentic account

4.2 Subsystem 2

The "General Information" subsystem is responsible for creating and continuously editing Facebook profiles. It excels in crafting profiles that are rich in authenticity, including the generation of names, profile pictures, personal information, and background details that resonate with the character of an elderly individual.

4.2.1 Assumptions

For this subsystem, there are also some assumptions to be made such as Human Oversight, Profile Consistency, and Data Privacy and Security. For the for first one, we need to assume that the profile creation and management process could involve some human oversight. We need to ensure that there is a change in events that reflects life events and experience. For the second assumption, we need to assume that the information remains consistent in terms of character portrayal. Any inconsistencies may result in compromise and suspicion. For the last assumption, we need to assume that the profile created appears realistic and authentic to potential scammers. General information is vital for this assumption as the information needs to be convincing enough to trap scammers and avoid suspicion.

4.2.2 Responsibilities

The "General Information" subsystem has key responsibilities in creating and maintaining convincing Facebook profiles for our fraud detection strategy. It generates authentic names, profile pictures, and personal information consistent with the character of elderly individuals. These profiles include background details to add depth and realism. The subsystem also manages privacy settings, balancing authenticity and security by configuring which information is visible to external parties. Regular monitor-

ing ensures profiles remain in alignment with character and privacy expectations. These tasks form the foundation for successful interactions within the fraud detection strategy.

4.2.3 Subsystem Interfaces

Table 3: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Information Input	Personal name Elderly age Martial status	Authentic info

5 Y Layer Subsystems

The Chatbot layer is composed of 2 sub systems which are Profile connection and Messages. The Chatbotâs task is to connect to the Facebook account of our persona and lure in scammers. Once the scammers have fallen into the honeypot, the Chatbot will begin to reply to the scammers while posing as an elderly person. Replies and messaging will be timed to avoid suspicion.

5.1 Subsystem 1 - Profile Connection

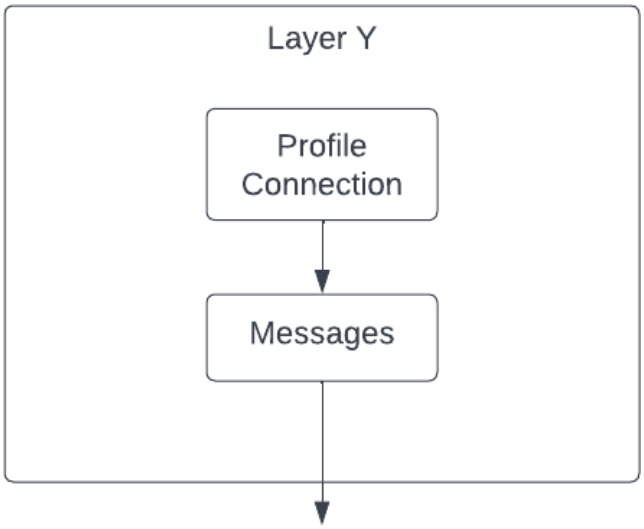

Figure 4: Example subsystem description diagram

5.1.1 Assumptions

For this subsystem we assume that the connection to the profile will provide all the information about the account that's necessary.

5.1.2 Responsibilities

This subsystem is responsible for connecting to a Facebook profile and takes on a crucial role in establishing a direct link between the Chatbot and the user's Facebook account. This intricate process involves a series of vital components. Initially, there's the Authentication and Authorization step, where the system verifies and grants the Chatbot access to the user's Facebook account, obtaining the necessary permissions for the Chatbot to operate on behalf of the user. Following this, the subsystem encompasses Profile Data Retrieval, which, once access is granted, empowers the Chatbot to gather information from the user's profile, including their name, profile picture, and any publicly available details. In addition, the Post and Profile Monitoring element continuously keeps tabs on the user's profile, scrutinizing it for new posts, updates, and changes, and may even collect relevant data about the user's interests and online behavior to ensure a comprehensive and responsive interaction.

5.1.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labelled interface that connects to this subsystem. For each entry, describe any incoming and outgoing

data elements will pass through this interface.

Table 4: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Connection to Facebook	Connection Request	Connection Status

5.2 Subsystem 2 - Messages

5.2.1 Assumptions

We assume that the Chatbot will access the inbox once booted up and will start following the instructions.

5.2.2 Responsibilities

The Messages subsystem is all about managing the messages that flow between the Chatbot and the Facebook user. This system involves a few critical parts. First, there's the Incoming Message Handling component, which kicks in when a user sends a message to the Chatbot. Its job is to figure out what the user is saying and what they want, which might involve understanding their language and recognizing their intent. After that, the Outgoing Message Composition takes over. This is where the Chatbot crafts a response to the user's message, which could be a written message, pictures, links, or other types of content to provide a helpful and engaging reply. Lastly, the "Message Delivery" component ensures that the Chatbot's response gets sent back to the user on Facebook, making sure the conversation keeps going smoothly.

5.2.3 Subsystem Interfaces

Table 5: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Inbox	Message in	Recieved Status
#2	Outbox	Message out	Delivered Status

6 Z Layer Subsystems

This section is dedicated to the Large Language Model integration into our code. This part of the code is basically like the brains of our chatbot. This layer will be interpreting whatever the user types to it plus whatever data/chat logs we may feed it.

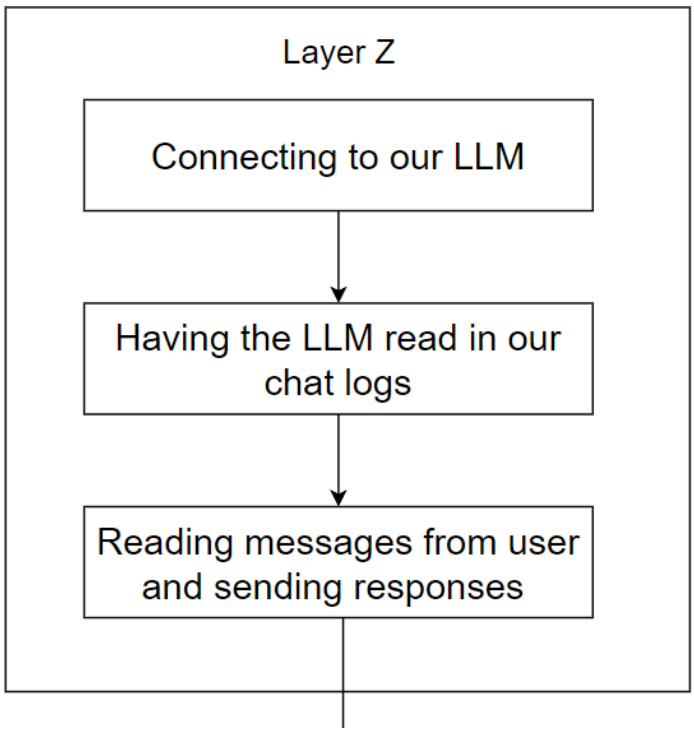

Figure 5: Overview of the subsystems of this layer

6.1 Connecting to our LLM

This section connects our code to our large language model. The other sublayers will be performing actions with the content imported here, thus information from here is communicated with the other 2 sublayers.

6.1.1 Assumptions

We are assuming the libraries for our subsystem are imported properly and we already have the libraries we need installed for our program to run. We are also assuming we are using the correct key to connect to our LLM account.

6.1.2 Responsibilities

This subsystem is first responsible for importing any libraries we may need to connect to the large language model. After that, we also need to input in the proper key so that our code can connect to the LLM account associated with our team. To use these large language models it typically costs some amount of money per message so that's why we would need an account and need to connect that account to our code.

6.1.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labelled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements will pass through this interface.

Table 6: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	This key connects our code to our account which connects us to the LLM	API Key	Error message if there was an error

6.2 Having the LLM read in our chat logs

We will need to train our bot using the large language model to act like a vulnerable widow. Now to do this the most accurate way we can we will feed our LLM any chats or data we may think may be useful. Importing this data and feeding it to our chat bot is what this section is dedicated to.

6.2.1 Assumptions

We are assuming we were able to connect to the LLM properly in the last layer with the proper API key and that our account has enough credit to process our message. We are assuming our LLM can process all our chat logs and data we are feeding it without any problems and have the bot act like how we wish for it to act.

6.2.2 Responsibilities

This subsystem is responsible for determining the behavior of the chatbot for the rest of the conversation. In this subsystem, the chat logs from a widow and a scammer will be fed into the LLM. Now this will be used later down the line since we want our chatbot to act similar to the widow from our chat and it will also analyze how the scammers talk in the chat logs and tell us if detects a scammer in any future conversations. Also, we directly instruct our LLM how to act before it starts analyzing the input from the user. For instance, we can directly tell our LLM to act like a grieving widow before any conversations start.

6.2.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labeled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements will pass through this interface.

Table 7: Subsystem interfaces

ID	Description	Inputs	Outputs
#2	These are the chat logs we will feed to our LLM to train it.	Chat logs	Nothing
#3	These are the commands we will issue to ChatGPT at the beginning to modify its behavior for the rest of its responses	ChatGPT instructions	Nothing

6.3 Reading messages from user and sending responses

This section of the code will interpret the message the user sends to it and give an appropriate response.

6.3.1 Assumptions

We are assuming we are connected to the LLM from the first step and that we provided sufficient chat logs and instructions to LLM so that it was acting as intended. But also identify scammers as intended from any suspicious messages received by any user. We are also assuming all chat logs with the user are kept so we can build on previous conversations.

6.3.2 Responsibilities

This subsystem is responsible for using the LLM after processing any chat logs and commands from the previous subsection to generate the appropriate responses whenever a user sends a message. Also, it is responsible for adding any of the conversations it has with any user to a database associated with each user, so it will remember each conversation it had with each user. So this subsystem is also responsible for feeding data into our large language model and keeping track of conversations.

6.3.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labeled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements will pass through this interface.

Table 8: Subsystem interfaces

ID	Description	Inputs	Outputs
#4	Our LLM will read in any input from the user and generate an appropriate response	User Input	Chatbot's response

7 A Layer Subsystems

The communication layer serves as a hub for managing message flow, interactions, and data exchange between the chatbot, external messaging platforms, and internal components. The communication is context-aware and provides smooth conversations between potential scammers and the bot. The subsystems for the layer include API calls, and message interactions with the bot, and the scammer. A more descriptive function of all of these subsystems is provided below.

7.1 Subsystem 1

API call - The API call subsystem is responsible for carrying out communication between the chatbot and external messaging platforms and services. It handles integration with the LLM API that generates chatbot responses.

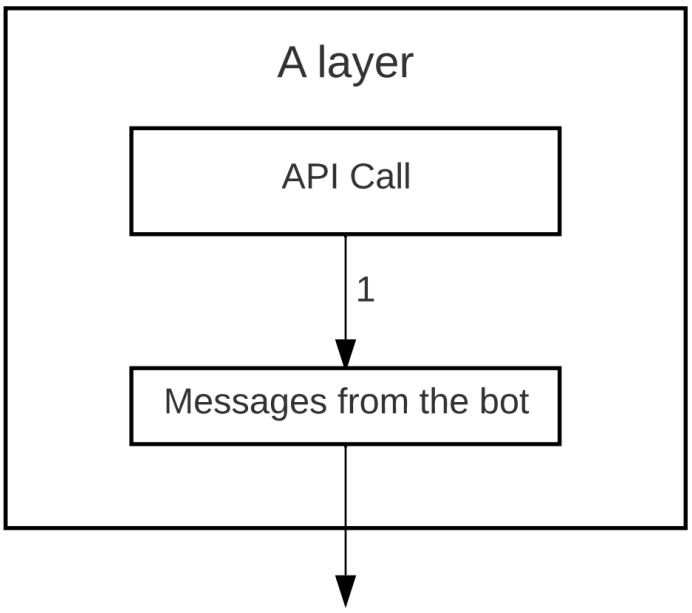

Figure 6: Subsystem description diagram

7.1.1 Assumptions

We are assuming that the external API has rate limits and usage policies that need to be adhered to. We are also assuming that the API call can successfully authenticate with the bot and can be used for our functions.

7.1.2 Responsibilities

- Message delivery based on incoming responses.
- Error handling and logging.
- Authentication with LLM code.

7.1.3 Subsystem Interfaces

Table 9: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	External API	Authentication credentials (API keys, tokens) outgoing generated messages	Incoming messages from external resources
#2	Resource management	Rate limit information for api	Resource allocated and provides rate limit
#3	Message content	Encryption keys to methods to secure content and metadata	Securely encrypts and decrypts ongoing messages

7.2 Message interactions from the bot

Message interactions from the bot - This subsystem is responsible for understanding the content and context of the incoming messages from the potential scammers to eventually send out appropriate responses to the scammers. This subsystem performs several essential functions such as storing messages and metadata that includes the timestamps, sender information, and any detected scammer indicators. Storing these data is crucial for auditing, reporting, and providing historical context for future messages. Another function is response speed which has to be subtle in a way that it doesn't raise any suspicion when the bot sends out a message. It has to mimic the response time of a legitimate conversation to maintain a natural appearance. Another function is to tactfully direct the potential scammers to send personal information about themselves. This would mean that the bot has to carefully craft messages to request specific information about the scammer without revealing its true intent.

7.2.1 Assumptions

It is assumed that the user interactions with the chatbot will adhere to ethical standards and that it doesn't contain any malicious elements.

7.2.2 Responsibilities

- Context management: maintain and update conversation context to provide relevant responses.
- Tailor responses based on past interaction and user-specified data.
- Monitoring and learning.

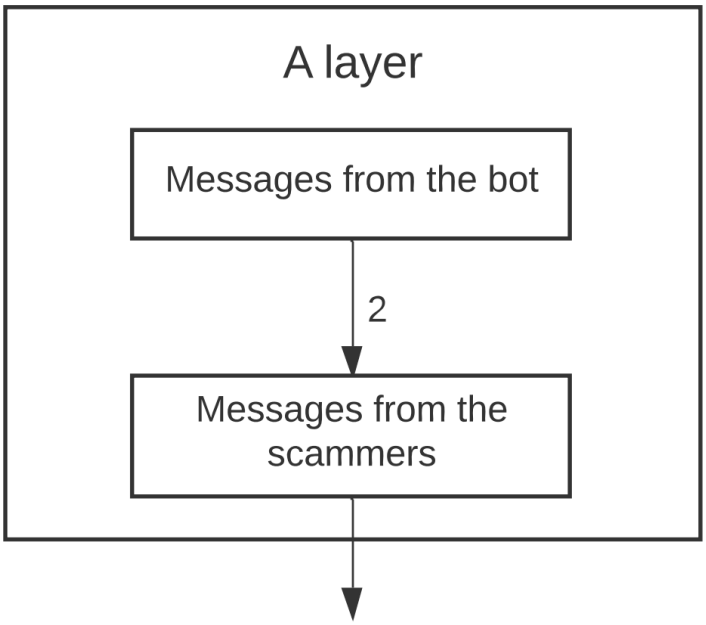

Figure 7: Subsystem description diagram

7.2.3 Subsystem Interfaces

Table 10: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Response Generation	User queries and messages, User preference and profiles	Crafted responses tailored to scammer's queries and conversations.
#2	Personalization	User profiles, preferences, personalization algorithms and models	Personalized contents or responses based on history
#3	Reporting and learning	Feeds suspicious behavior data	Insights and data for continuous strategy to trap the scammer

7.3 Subsystem 3

Message interactions from scammers - This subsystem is responsible for monitoring messages to detect any suspicious patterns, keywords, or behavior that suggest fraudulent intent. The messages will be securely stored as metadata to be used for future conversations and references.

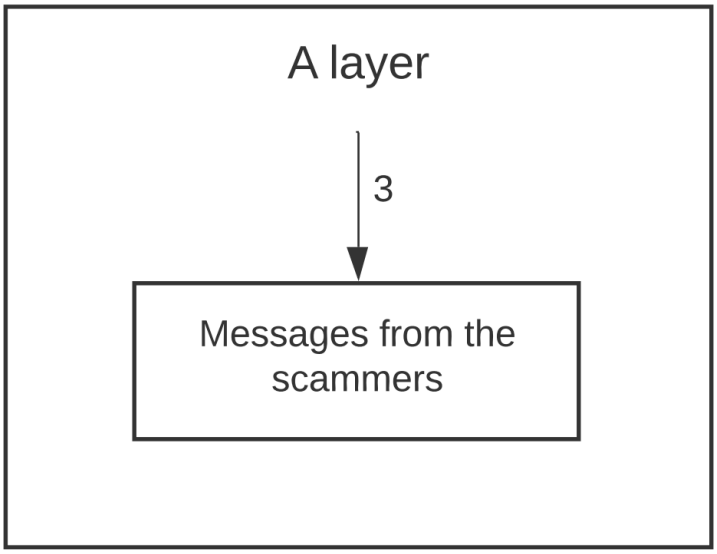

Figure 8: Subsystem description diagram

7.3.1 Assumptions

It is assumed that the subsystem is capable of making real-time decisions regarding response strategies and escalation when engaging with potential scammers. It is also assumed that the bot interaction with the scammer will be initiated by the scammer in the beginning.

7.3.2 Responsibilities

- Deceptive behavior recognition
- Message Analysis and monitoring
- Escalation and reporting

7.3.3 Subsystem Interfaces

Table 11: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	Message Analysis	Text, media and metadata from messages	Data logs and reports on detected scam indicators
#2	Escalation and Reporting	Criteria and thresholds for identifying escalated situations	Detailed reports and records of potential scam activities

8 B Layer Subsystems

In the Reporting System Layer, the actions that will be taken after a scammer has been identified are done. There are 2 subsystems in this layer the Automated Reporting System and the Scammer Database we are building. The Automated Reporting System will automatically file any reports we need to make with the information given to it from the Chatbot control part of the code. While the scammer database is a database we are building of confirmed scammer profile which we will release to the public to warn others. Now first we will add a scammer to the scammer database and after that, we will file any police reports or any reports to Facebook.

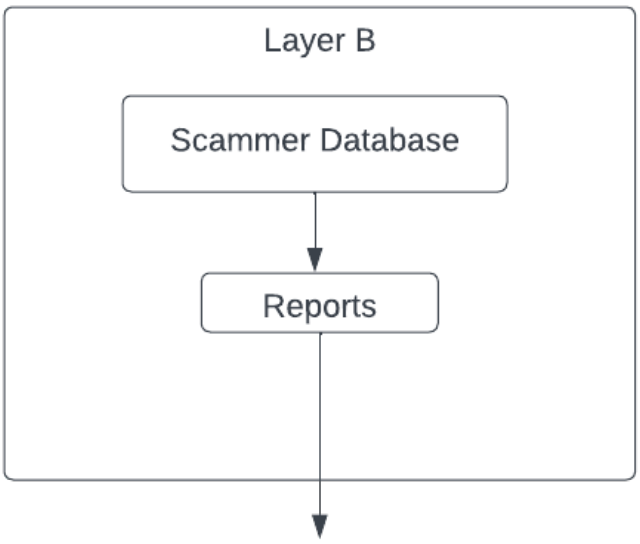

Figure 9: Example subsystem description diagram

8.1 Automated reporting system

This section is focused on the code related to automatically filing police reports and reporting Facebook accounts after we verified that someone is a scammer.

8.1.1 Assumptions

We are assuming the person who has been identified as a scammer is in fact a scammer. Also, the chat logs given to us from the Chatbot control layer are incriminating and the proper information of the user has also been acquired from the Chatbot control layer.

8.1.2 Responsibilities

This subsystem is responsible for automatically reporting the user's account to Facebook for running a scam, hopefully this will lead to their account being terminated. But also automatically filing a police report too, with the incriminating chat logs as evidence and with the user's information from their Facebook profile. It is also responsible for filing this police report properly, if we were to do it improperly we might be wasting the police's time and we have to make sure everything is tested rigorously before any of this is implemented.

8.1.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labeled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements that will pass through this interface.

Table 12: Subsystem interfaces

ID	Description	Inputs	Outputs
#1	The information here is submitted to a police report, which will take any incriminating chat logs and the user's information from their Facebook profile	chat logs user's profile information	A successfully created police report
#2	The information here is submitted to report an account to Facebook themselves	user's profile information	A successfully filed report to Facebook

8.2 Scammer database

This section will add the confirmed scammers to our scammer database and share this database with the public.

8.2.1 Assumptions

Again like the last subsection stated, we are assuming the user whom we are adding to the scammer database is in fact a scammer. We are assuming the verification done in the other layers for whether the user is a scammer or not was done properly.

8.2.2 Responsibilities

This subsystem is responsible for automatically creating new entries in our confirmed scammer database after a scammer has been identified in the other layers. This subsystem is also responsible for parsing the right information to the database from the information passed to it from other layers. This subsystem is also responsible for making this database be visible to the public, whether it by us making a website to record all these scammers or we could make a Facebook page to record all the confirmed scammers. The process of making this information be public is another responsibility.

8.2.3 Subsystem Interfaces

Each of the inputs and outputs for the subsystem are defined here. Create a table with an entry for each labeled interface that connects to this subsystem. For each entry, describe any incoming and outgoing data elements will pass through this interface.

Table 13: Subsystem interfaces

ID	Description	Inputs	Outputs
#3	This is the information we are using to add a scammer's account to the confirmed scammer database.	user's profile information	A new successfully created entry in our scammer database

9 C Layer Subsystems

In this section, the layer is described in some detail in terms of its specific subsystems. Describe each of the layers and its subsystems in a separate chapter/major subsection of this document. The content of each subsystem description should be similar. Include in this section any special considerations and/or trade-offs considered for the approach you have chosen. This is the Web Scraping tool used to identify vulnerable people on facebook by analyzing profiles and using a specific criteria such as age and posting patterns to help us identify the types of people who are vulnerble. The tool will also search facebook to find potential scammers where a different criteria will be used. Posting patterns and keywords that exhibit scamming behavior will be analyzed in an effort to help understand how scammers operate as well as to generate a list or report of potential scammers for further analysis to validate them.

9.1 Subsystem 1

This section provides a detailed overview of the Vulnerable Profile Detection subsystem, a crucial part of the Web Scraping and Analysis Layer. It explains how the subsystem processes Facebook profiles to identify potentially vulnerable individuals and communicates with the Web Scraping Tool.

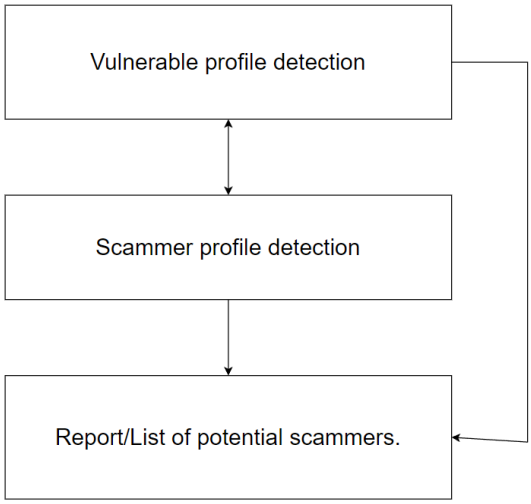

Figure 10: Example subsystem description diagram

9.1.1 Assumptions

Assumptions include access to Facebook profiles via authorized APIs, availability of relevant user data (age, engagement patterns), capability to identify vulnerable users based on behavioral analysis, and adherence to legal and ethical standards in data usage for vulnerability assessment.

9.1.2 Responsibilities

The system analyzes user profiles, posts, and interactions, employing algorithms to assess behavior and engagement patterns indicating vulnerability.

9.1.3 Subsystem Interfaces

Table 14: Subsystem interfaces

ID	Description	Inputs	Outputs
#01	It defines the interfaces connecting the Vulnerable Profile Detection subsystem with the Web Scraping Tool.	Receives Facebook profile data for vulnerability analysis.	Sends detected vulnerable profiles to the Reporting Module.

9.2 Subsystem 2

The Scammer Profile Detection subsystem focuses on identifying suspicious Facebook profiles that exhibit patterns indicative of scamming activities. It employs natural language processing and machine learning techniques to analyze messaging content and user behavior, flagging potential scammers for further investigation.

9.2.1 Assumptions

Assumptions include authorized access to Facebook messages and profiles via APIs, availability of message content and metadata for analysis, ability to identify scam-related keywords and patterns, and ensuring legal and ethical use of message data for scammer detection.

9.2.2 Responsibilities

The system analyzes profile content for scam-related keywords and language patterns, utilizing machine learning algorithms to identify scammer-like behavior. Suspicious profiles engaging in scam-related conversations are flagged for further scrutiny.

9.2.3 Subsystem Interfaces

Table 15: Subsystem interfaces

ID	Description	Inputs	Outputs
#02	It describes the interfaces connecting the Scammer Profile Detection subsystem with the Web Scraping Tool.	Provides Facebook profile data and keywords for scammer analysis.	Sends detected potential scammers to the Reporting Module and the Chatbot Module.

9.3 Subsystem 3

The Generate List of Potential Scammers subsystem compiles and maintains a comprehensive list of identified potential scammers. It stores relevant information, including profile data, message history, and flagged scam attempts. This subsystem ensures that the collected data is organized, updated, and ready for analysis, facilitating the reporting process.

9.3.1 Assumptions

Assumed availability of secure storage resources for maintaining a list of potential scammers, including profile data and flagged scam attempts. Assumed regular updates and maintenance of the list as new scammers are detected. Legal and ethical considerations are assumed in the secure storage and usage of scam-related data for reporting purposes.

9.3.2 Responsibilities

Compile a detailed list of potential scammers, including relevant profile information and conversation transcripts. Store flagged scam attempts and identified scammer profiles securely. Ensure the list is regularly updated and maintained as new potential scammers are identified through continuous operations.

9.3.3 Subsystem Interfaces

Table 16: Subsystem interfaces

ID	Description	Inputs	Outputs
#03	It defines the interfaces connecting the Generate List of Potential Scammers subsystem with the Web Scraping Tool and the Reporting Module.	input 1: Provides data of potential scammers for storage and documentation. input 2: Receives the compiled list of potential scammers for further analysis and reporting.	output 1: Sends updated scammer list to the Reporting Module for analysis. output 2: Provides insights and reports based on the analyzed scammer data.

References