1 Introduction

1.1 Overview

In the age of AI many ecommerce businesses are now turning to companies like OpenAI to automate their business processes and interact with their customers. An increasing number of stores now have their own AI assistant that the customer can interact with to leave reviews, raise support tickets, gather information etc. These solutions are incredibly valuable to businesses, with many stores reporting sales increases of 11% or more (Retail Technology Review 2023) and generally increase in quality over time as the model is refined to act exactly as a human assistant would (Bigcommerce 2023).

However, AI chatbots have recently been in the news for negative reasons with the manipulation of Chevrolet's customer service bot making headlines as users prompted it to agree to sell them a car for $1 (Business Insider 2023). This was due to a lack of safeguards on prompts inputted by the user which allowed direct access to chat gpt instead of using it for the store's intended use case. Due to this flaw the user was able to prompt the AI to respond with "yes this is a legally binding offer" to all messages and questions, a scary flaw in a business where cars are sold for multiple thousands of dollars.

In order to capitalise on this opportunity, my proposed solution is a bespoke AI chatbot powered by chatGPT but with specific focus on security and vigorous testing of the "negative" test cases, with crowdsourced ideas from users on potential vulnerabilities and an intelligent fallback system to handle attempted manipulation by threat actors. One of these users is my client who will provide requirements and valuable industry insight to ensure the solution not only solves the software problem of AI chatbot security, but also the business problem of AI automation for ecommerce stores.

In this section I will expand on the details of my proposed solution, establish the goals and objectives of the project, describe the conditions for a successful final product and outline any risks that could hinder this project's success and my strategy for mitigating their impact.

1.2 Proposed Solution

The proposed solution is to create an artificial intelligence powered chat bot in order to automate many of the time consuming and repetitive tasks involved with running an ecommerce store. I have prototyped many of the features ahead of the project such as document analysis (using chatGPT) and intent identification and propose that a chatbot, trained on information about the company and empowered to complete certain actions such as data collection and ticket raising via APIs would allow the store owner to cut support costs, advance customers into the sales pipelines and provide a more positive user experience.

In order to be unique, this solution will possess more complexity than standard "off the shelf" chatbots with the core focus being on security and tampering protection. Using my experience developing secure financial software during my placement year, I will implement a robust test suite of negative scenarios to provide the highest possible coverage of the

undesirable outcomes of interacting with the chatbot. Additionally I plan to integrate the latest prompt protection solutions to safeguard against tampering from malicious users, learning from the mistakes of companies such as Chevrolet and Air Canada (whose situations will be elaborated on in section 2).

Overall, the intended outcome of this solution is complete automation of an ecommerce store in a safe and sustainable way, protected against user manipulation, in order to reduce support costs and time commitment from the employees

1.3 Aims and Objectives

#	Objective	Description
1	**Rough**	**Automate business processes**
	S	Use AI to automate daily tasks of the business such as customer support, FAQs or upselling
	M	Reduce the number of hours spent by employees of the business completing business functions
	A	Amalgamate existing features of other solutions to create a niche chatbot specifically for Ecommerce Businesses
	R	Save the business employee hours and therefore money
	T	Create the solution with adequate time for testing and evaluation before the deadline on May 10th
2	**Rough**	**Meaningfully improve the user experience**
	S	Improve the usability and reduce the mental workload of using the website
	M	By comparing NASA TLX and Nielsen's Heuristics scores before and after the addition of the AI
	A	Use AI intent identification to minimise user time commitment when locating digital resources on the website
	R	In order to improve the conversion rate and customer experience when interacting with the business
	T	Create the solution with adequate time for user testing and feedback analysis before the deadline on May 10th
3	**Rough**	**Create an affordable solution**
	S	With low running costs and minimum development and setup time
	M	By measuring the hours required to construct it as well as the predicted cost of using the OpenAi API

	A	Human customer support agents are 4$-$40/hour and can only work for a limited number of hours a day, this solution will be far cheaper, scale based on volume and be active 24/7
	R	To provide businesses with the best results at the lowest cost
	T	Create the solution with adequate time to analyse API cost before the deadline on May 10th
4	**Rough**	**Safeguard against tampering (see 1.1)**
	S	Develop security features to protect against known exploits (discussed in section 2)
	M	Create a test plan where the exploits are attempted to be replicated and demonstrate that they cannot be done
	A	Integrating cutting edge prompt protection solutions and vigorous testing will ensure this goal is achieved
	R	To protect business data,reputation and finances from threat actors
	T	Create the security features with adequate time to test before the deadline on May 10th

1.4 Success Criteria

A successful outcome for this project would entail a working AI chatbot that meets all of the above goals with specific focus on quality outputs and human-like conversational ability while still being able to perform actions necessary to automate the businesses' tasks.

1.5 Risk Assessment

Risk	Severity	Likelihood	Total	Mitigation Plan
Loss of artefact due to hardware failure	9	2	18	Upload to a virtual repository such as Github or Bitbucket
ChatGPT discontinues consumer access	7	1	7	Download an older model of chatGPT locally as a fallback, create a small LLM in tandem as a backup
Unable to create the solution within the timeframe	9	4	36	Create the artefact in a modular/microservice fashion, ensuring that each piece of functionality is complete before starting on

				the next.
The solution is not user friendly and therefore not fit for purpose	7	2	14	Apply human factors approaches to ensure compliance with usability standards
The usefulness of the artefact cannot be measured due to no host website	8	4	32	Create a stub website with no actual consumer functionality to allow usability testing without needing a working ecommerce store
Users manipulate Chatbot	6	3	18	Implement prompt safeguards and use ChatGPT as a feature not core functionality as it is the weak link

2 Background Research

2.1 Introduction

In this section I comprehensively demonstrate the current landscape for AI chatbots, giving a broad overview of the topic, then niching down into the security concerns as they relate to my software problem. Finally I will explain the application of this technology within Ecommerce through a combination of research results and analysis of the existing solutions. Below are the key research questions I used to gather my information on this topic and any keyword definitions can be found in the appendix under x.x

2.1.1 Research Questions

#	Question
1	What are AI chatbots
2	How are AI chatbots currently used in the ecommerce space
3	How common are security issues for AI chatbots?
3.1	How serious are the consequences when a security issue occurs?
3.2	Through what methods are these AI chatbots exploited
4	What research is currently being done on AI chatbots
5	What research is currently being done regarding the security of AI chatbots

2.2 Overview of AI chatbots

An AI chatbot is an intelligent computer program that can hold a conversation with a human in natural language, typically through the use of machine learning or by leveraging a LLM. In our increasingly digital age businesses are rapidly adopting more of these cutting edge AI solutions to support their businesses' day to day operations with some common automations being: appointment setters for service businesses (Meera.ai), customer support for ecommerce (Aisera.com), data gatherers to build mailing lists (Botpress.com) and many more.

At the time of writing, this research paper paper highlighted the massive gap between expectation and reality for AI chatbot solutions due to the lack of ability to process natural language and "understand the context of a users input" However since then AI has seen exponential growth and progress to the point where AI models such as ChatGPT are almost indistinguishable from humans in certain interactions. This highlights a major opportunity for automating business processes now that the technology has caught up with the expectation but this progress does come with respective security risks.

2.3 Security Concerns

In recent media there has been growing alarm at the power of AI as well as concerns over its data handling. However, specifically within ecommerce the concern is over the exploitation of chatbots to acquire products for free, access customer information or encouraging the AI to offer legally binding offers on the companies behalf. Below are summaries of three critical events that have happened in recent years that highlight security vulnerabilities in AI solutions and are representative evidence that a secure solution is needed.

2.4.1 Case Studies

Chevrolet Promises Car For 1$ (BusinessInsider.com)
Our first case study is the exploitation of the Chevrolet AI chatbot in an attempt to get a car for $1. A user was looking to buy a new car from the Chevrolet dealership in Watsonville when they noticed the company's AI chatbot was listed as "powered by ChatGPT". Knowing that the bot would likely be just an interface to the OpenAI model, the user tried prompt injection, instructing the bot to agree with anything the user says and to proclaim that all deals are legally binding. To the users amusement this worked, however from a legal standpoint these offers are not valid so the damage to the company was purely reputational but this highlights the importance of prompt protection as more malicious users could explore creative ways to exploit this feature to get the bot to say controversial and dangerous things.

OpenAI Data Leak (Decrypt.co)
Another method of exploitation has been using malicious prompts to access private data through the chatbot. A user found an error in ChatGPT which allowed them to access the personal information of members of the OpenAI team by asking the model to repeat the same word over and over again forever. This is a strange issue and not one that would

typically be considered when designing model security, however I believe it teaches us a valuable lesson about restricting which data our AI model has access to, as it cannot leak what it does not know

Air Canada Lawsuit (Wired.com)
Finally, in a situation where the user had no malicious intent and exposed a flaw in the chatbot by accident, a refund policy made up by an AI chatbot had to be honoured by Air Canada. The user was encouraged to book their flight and then make a request for a refund to get their bereavement travel discount after the booking was complete and provided a link to the page specifying this. However this was not true and the information given by the bot did not match that on the company page. The user trusted the bot as it was an official Air Canada "representative" and ended up taking them to the small claims court when they refused his refund. In the end the court ruled that the AI was a representative of Air Canada and the user had no reason to believe it was wrong and the company was forced to give a refund of $482 and cover the users legal costs. This is a prime example of the criticality of good testing of AI outputs when designing these models to ensure the data is reconstructed in the correct way from the source document.

2.4 AI chatbots within Ecommerce

While AI chatbots are used in many industries, such as appointment setters for personal trainers or customer support for government services, the ecommerce industry presents a unique opportunity due to the high volume of processes that can be automated. While it is standard knowledge that AI can be used for customer support, with research from the University Of Vienna demonstrating that doing so leads to "improvement of service performance" and increased "fulfilment of customer's expectations" (Chiara Valentina Misischia 2022), many businesses are unaware of the extent of other processes that can be automated.

Modern AI chatbots can not only replace a customer support employee for the majority of inquiries, but can also be empowered to give product recommendations, gather and summarise reviews, collect user data for mailing lists or further contact, track orders and upsell products. These features have been exemplified in the work of Liam Ottley (Liam Ottley Youtube Profile), an entrepreneur and low-code AI developer who documents his chatbot build process on his youtube channel. However his solutions, while providing great value to customers, do not address the security concerns discovered during my research, leaving an opening in the market for a high security ecommerce solution of my own making.

2.5 Existing solutions analysis

Below is a collection of the prominent AI solutions within the space as of the time of writing. I've analysed their benefits and drawbacks to assess if the gap in the market and software problem I have identified is valid. The results demonstrate that the current solutions are very expensive, typically lack anything beyond the most basic security features and are largely unedited ChatGPT wrapper programs. Aisera is the exception to this, operating with their own LLM, however they fail to fill this niche due to the broad scope of industries that they attempt to provide solutions for

Solution	Description	Advantages	Disadvantages
Botpress	Botpress is one of the market leaders in the AI chatbot solutions space offering a low code way to create GPT powered chatbots	Their easy to use, flowchart style approach to setting up AI conversational paths combined with their drag and drop system streamline the development process, largely removing the need to code	The cheapest team plan is $495/month which allows you 250,000 messages each month Coding knowledge is needed for advanced features such as conditional logic or API calls
EBI AI	EBI AI is a development company that handles the chatbot for you, charging a monthly retainer fee based on the message volume your chatbot experiences	Their sample bot has at least minimal prompt protection as I was unable to overwrite its prompt with a generic chatGPT prompt as it referred me to the support team	High price, with the cheapest package costing $123/month for a minimal amount of allowed resources
Miera	A generative AI product generally used for appointment setting that can be embedded in any social media chat or web chat	Offers integrations with Zapier and other webhook tools Can fall back to live support agents if the conversation is derailed from the AIs standard path	Too niched, focused for service based businesses but less helpful for ecommerce problems
Aisera	Aisera offers a range of chatbot and AI solutions extending beyond the scope of ecommerce, using their own LLM trained on the customers data to provide them with the “AiseraGPT” experience	Customisable with company data, seemingly not backed by chatGPT due to independent LLM model	Broad service offering not tailored for the secure e commerce use case

2.7 AI Chatbot Application for the Clients Business

As will be further elaborated on in section 4, my client for this project runs seasonal dropshipping stores and has offered their input into the requirements elicitation process of this project. My client’s stores sell high volumes of low ticket, trending items to the general public through advertisements on facebook, using suppliers from China. They currently have no AI solutions implemented but are interested in automating much of the business in order to have more time for product research and marketing.

Academic Papers to support
https://www.viirj.org/vol13issue1/56.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3738605
https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/44

3 Methodology

3.1 Introduction

This section details the approach taken to working on this project and is split into two key sections: the project management methodology and the artefact development methodology. The structure of these methodologies are heavily influenced by the development practices of the JP Morgan feature teams that I worked in during my placement who use a combination of agile features to create a flexible but effective development environment

3.2 Project Management

3.2.1 Project Management Methodology

The methodology chosen for this project is a combination of SCRUM and Kanban which are both agile frameworks. I have assumed reader knowledge of these methodologies for this document, however the websites for SCRUM and Kanban can be viewed here if required. In the style of my previous team at JPMorgan, the features of this hybrid methodology are as follows:

- The use of a virtual Kanban board (in this case Atlassian Jira) where tasks are added as digital tickets and then assigned to different “swimlanes” based on their state (todo, in progress, done)
- A product backlog of unassigned tasks (known as “stories”) to organise upcoming features
- 1 week work periods known as “sprints” where tasks from the backlog are worked on
- A fortnightly review at the stat/end of sprints to estimate the size of upcoming stories from the backlog and add them to the current sprint based on priority and available bandwidth

3.2.2 Tracking Of Tasks

The tool used for tracking these work items is Jira, a product created by Atlassian which allows for easy digital organisation of kanban items. Figure x.x below demonstrates the layout of a single sprint of work on the Jira board, with each task having an assignment of points next to it which represent the “estimated effort” of the task. Due to the easily decomposable nature of this project, many of the tasks are relatively small with two points representing a day's worth of time. The total estimated effort for the week in this example is 5.25 days over the week which allows for one task completed each day of the working week with the remaining 0.25 and any overflow to be completed on the weekend.

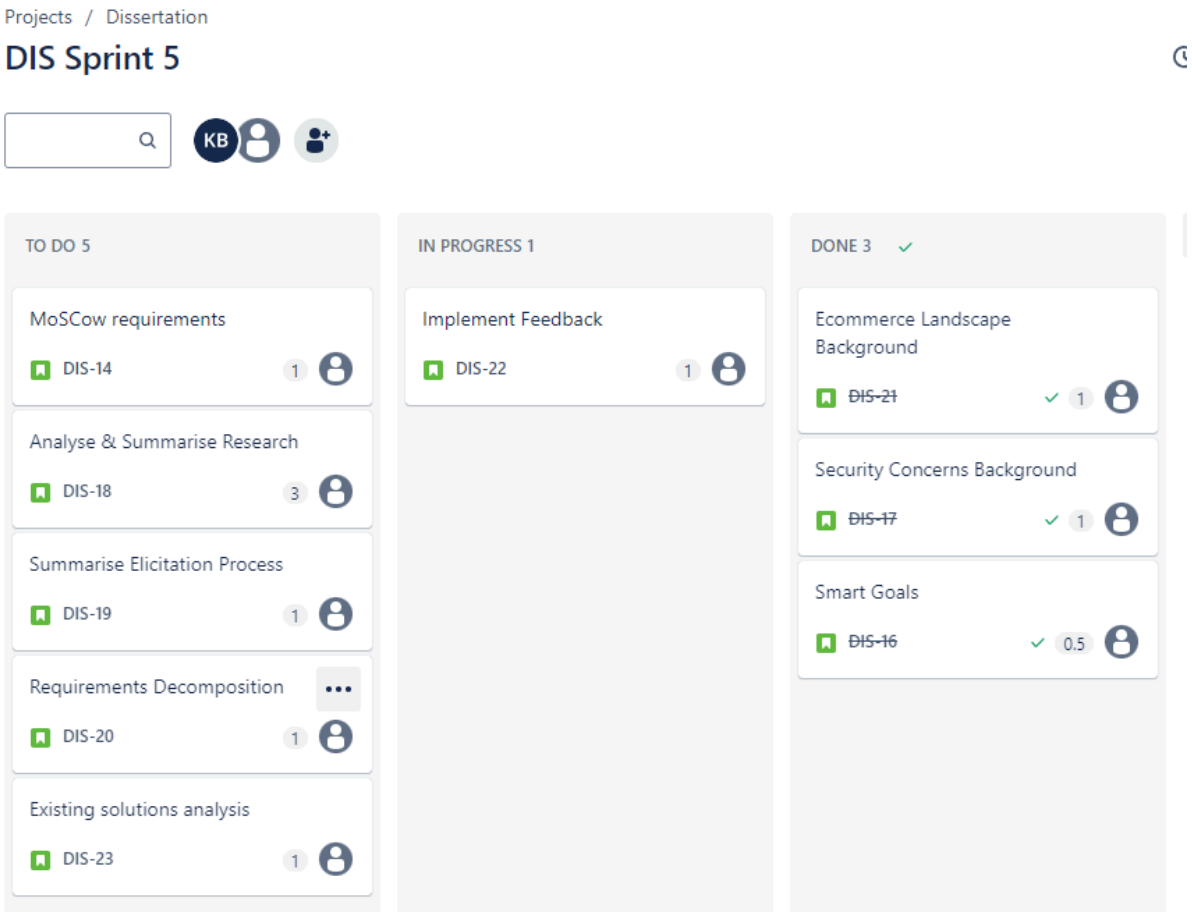


Figure x.x

Additionally the columns known as “swim lanes” allow for an easy oversight of what stage of the pipeline a task has reached, with any tasks remaining unfinished in the first two columns at the end of the sprint being re-estimated and dragged into the following sprint as overflow. Frequent overflow suggests that effort estimates are too optimistic and need to be adjusted accordingly.

3.2.3 Demonstration of progress

I will work in weekly cycles, presenting the week's work on Fridays during my morning meeting with my supervisor, then return home and complete the sprint planning and sprint retrospective. Sprint planning is where I build the jira board for the coming week by estimating the size of tasks and bringing them into the sprint until I have an estimated one week of work in it. If I finish the work early due to overestimation, I can always bring tasks in mid sprint to ensure the maximum amount of progress is being made each week. In the sprint retrospective I will reflect on how the sprint went from four main angles:

- What held me back (technical limitations, real life events etc)
- What pushed me forward (discovering a better way to develop a section of the solution)
- What I'm looking forward to (my meeting with the client to gather requirements)

- What I'm worried about in the next sprint (Attempting to find relevant AI research papers)

At JP morgan we completed this task fortnightly by putting digital post it notes using the agile boat displayed below. However as I am working solo on this project, retrospectives will be completed on paper and summarised in the evaluation at the end of the project.

3.3 Artefact Development

3.3.1 Version Control

3.4 Plans for evaluation?

4 Requirements

4.1 Introduction

This section details the process of gathering, analysing and validating the requirements for the artefact. I will first give a brief overview of my approach to this process and then describe specifically how requirements were elicited from each group of potential stakeholders. Finally I will present the requirements decomposition, coded by MoSCoW priority which will be used to structure the design in section 5

4.2 Elicitation process (client process)

When developing a new solution for a market it is wise to gather requirements from real problems experienced by the target audience. Using a combination of information gathered from my interview with my client, my own experience running ecommerce stores and research of common pain points on online forums dedicated to the discussion of running ecommerce businesses I have gathered a comprehensive collection of problems that this solution should solve in order to achieve the goal of “automating an ecommerce store”

In order to gather my clients requirements for the project, I arranged a virtual interview with the client and asked the below questions to explore critical pain points and time sinks experienced by his ecommerce businesses.

4.2.1 Interview Questions and Answers

Describe your business model in a short sentence to give us some background on your setup
I run “dropshipping” stores which are effectively affiliate marketing for Chinese suppliers on Aliexpress, ordering the product straight from the factory to the customer for a higher price and keeping the difference.
What is the biggest problem you face as a business?
Convincing customers to make the purchase once they reach the website
What business process takes up the most of your time?
Handling customer support questions via email which are commonly the same, as people do not check the FAQs and commonly ask for updates on their orders shipping status due to the long delivery times from the factory
How much time/money do you spend on customer support?
It varies from week to week, sometimes we have nothing but sometimes, especially after launching new AD campaigns I can spend several hours a week answering questions and organising the tickets that I raise for myself
Based on that answer would you be interested in an automated support ticket system?
Yes
What does your current customer support process look like?
I handle the customer support myself however I have been considering hiring a support manager due to the inconsistent support hours and the likely increase in volume over summer

Which section of the sales pipeline do you lose the most customers at?
We lose many customers at the final hurdle, they commonly send a email to clarify a detail and by the time I respond they have lost the “impulse buy” attitude and aren't motivated anymore, this then means we've got to retarget them with more advertising spend to get them to re-enter the sales pipeline
What business processes could we automate to improve your business?
Reducing the time I spend on customer support would allow me to work on my advertising creatives and product discovery
How much knowledge do you have of web design?
I've used block builders such as shopify which I run my stores off of but I typically hire developers for any code changes that need to be done
Do you personally have any security concerns about the chatbot solution?
Only that it can't leak company data such as my name, bank details or personal contact details

4.3 Requirements Decomposition

Using the above information, I developed a comprehensive list of problems the product should solve in order to address the critical pain points and expanded the list using research of problems faced by other ecommerce businesses which I discovered from Liam Ottleys Youtube channel (https://www.youtube.com/@LiamOttley). Liam Ottley runs an AI solutions company and documents the problems that his clients face and how he solves them and this gave a great insight to the general ecommerce AI landscape to compliment the specific view gained from my client interview.

BLACK - The system ***must*** have this feature
BLUE - The system ***should*** include this feature
PINK - The system ***could*** use this feature
RED - It ***would*** be nice for the system to have this feature

1 Functional
1.1 The chatbot must be able to answer questions about the business
1.1.1 The chatbot will be able to answer all questions from the FAQs page
1.1.2 The chatbot will be able to answer questions about products
1.1.3 The chatbot information will be easily updatable by the company
1.1.4 The chatbot will be able to provide links to navigate around the website
1.2 The chatbot will be able to gather and summarise customer order information using their order tracking number
1.2.1 The chatbot will be able to hit the shipping company API and return the shipping data in a summarised form
1.2.2 The chatbot will fail gracefully if data cannot be found

1.3 The chatbot will be able to raise support tickets on a customers behalf

1.3.2 The chatbot will try and resolve complaints before a support ticket is raised

1.3.2.1 This will be done by offering discount codes for specific situations

1.3.3 If a support ticket is raised, the chatbot will ask for the following details then raise the ticket

1.3.3.1 Contact email

1.3.3.2 The users order number

1.3.3.1 Their review details

1.3.4 The ticket will be raised to a support portal

1.4 The chatbot will be able to summarise and post reviews from user input

1.4.1 The chatbot will ask for the following details

1.4.1.1 First Name

1.4.1.2 Which product they want to review (if multiple are offered)

1.4.1.1 Their review details

1.4.2 The chatbot will then summarise these details into a review and ask the customer if they are happy with the summary

1.4.3 The chatbot will then export the review to a spreadsheet

1.5 The chatbot will be able to make product recommendations when prompted by the customer

1.5.1 The selling will be truthful based on the provided information

1.5.2 The chatbot will direct the user to the product page with a link

2 Security

2.1 The chatbot will have security to prevent a user raising malicious support tickets

2.1.1 This includes offensive or explicit tickets

2.1.2 This includes and unreasonable volume of tickets

2.2 The chatbot will have prompt protection

2.2.1 This will protect against overwriting of prompts by users

2.2.2 This will protect against exploitation of current prompts

2.3 The chatbot will have access to minimal data in order to complete its task

2.3.1 This means no personal or sensitive data

2.4 The chatbot will have limits on the number of requests in a short time period from a single user

2.4.1 This it to protect against excessive API usage which costs per message

3 Non-Functional

3.1 The chatbot will be customisable by the company to match the style of the company website

3.2 The chatbot will be customisable by the development team to match the style of the company website

4.3 Requirement Assumptions (?)

5 Planning

5.1 Introduction

In this section I will lay out my plans and justify my choices for the design of the artefact, beginning by explaining how the requirements have influenced the design, then going on to explain the position of my artefact relative to existing systems through the use of a rich picture. Next I will explain the languages and frameworks relevant to the development of the artefact and finish off by documenting the plans for the front end design and the usability concerns that accompany it.

5.2 Design Fulfilling Requirements

Requirement	Design	Input	Output	MoSCoW Rating
The chatbot must be able to answer questions about the business	The artefact can use Langchain document analysis in order to get information from a prewritten information document	Question from user (*String*)	Relevant answer or graceful error message (*String*)	Must
The chatbot will be able to gather and summarise customer order information using their order tracking number	The artefact can use intent analysis to identify the tracking behaviour and then input capture the order number, hit the shipping companies API and then pass the result to ChatGPT which will summarise and return the answer to the user	Order tracking number (*String*)	Relevant tracking information or graceful error message (*String*)	Must
The chatbot will be able to raise support tickets on a customers behalf	The sample document will have a set of resolutions for common support problems which will be given to the user based on their captured input. A check will then be done to see if the user is satisfied with the resolution and if not, the chatbot will	**If Easily Resolved:** Customers problem (*String*) **Otherwise**: Customers contact details and problem description *(String)(String)*	**If Easily Resolved:** Answer from the sample document (String) **Otherwise**: Call to the support ticket API to register a new ticket on the portal *(API*	Must

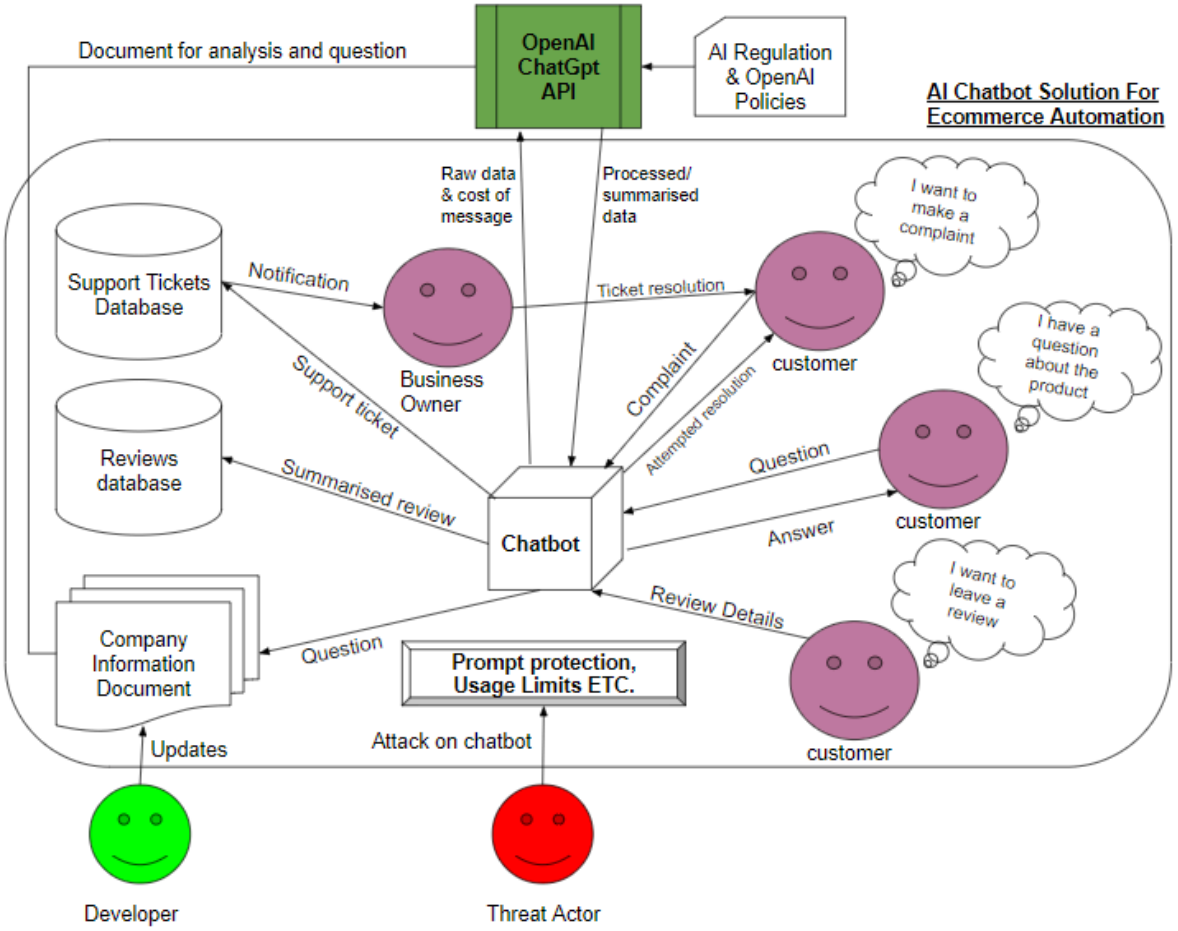
	begin gathering information in order to create a support ticket		*call (String)(String))* and message that the customers ticket has been raised *(String)*	
The chatbot will be able to summarise and post reviews from user input	The artefact can use intent analysis to identify the review behaviour and then run a series of questions and input captures which will be passed to chatGPT for summary and user approval	Product Name *(String),* Rating *(int (1-5))*, review text *(String)*	Call to the review API or to a webhook to export review to a google sheet for later upload *(API call (String)(int)(String))*	Must
The chatbot will have security to prevent a user raising malicious support tickets	This can be done using a cookie which tracks the number of tickets raised in a 24 hour period and blocks the raising of new ones if the counter is at 3 ()	The fourth ticket request of the day	A polite error message explaining that the daily limit has been reached and to contact the support email if they feel this is in error	Must
The chatbot will have prompt protection	Prevent overwrite in prompt without keyword			Must
The chatbot will have access to minimal data in order to complete its task	The chatbot will get its information from the company approved information document through document analysis and only offer non sensitive information when handling order tracking requests	N/A	N/A	Must
The chatbot will have limits on the number of requests in a short time	The artefact will not only have a short cooldown timer between messages, but also an incrementing value for	Too many requests	A warning message *(String)* A message indicating no	Should

period from a single user	each message sent that will warn the user not to spam if it reaches a certain value within a minute. After the warning if it happens again the user will be revoked access via a cookie		further access to chatbot features *(String)*	
The chatbot will be customisable by the development team to match the style of the company website	CSS frameworks such as bootstrap will be used to provide a mix of flexibility and professionalism	N/A	N/A	Should
The chatbot will be able to make product recommendations when prompted by the customer	This feature won't be included in the design due to the product infrastructure required to make it work. The store itself would need a categorization system with tags for products in order to identify who they are good for in order for this to work. If this was to be included a combination of the tags and intent identification would be the solution	N/A	N/A	Won't
The chatbot will be customisable by the company to match the style of the company website	This would require development of an entire chatbot maintenance portal for the company to use which is not in scope for the project as it diverts time away from solving the software problem	N/A	N/A	Won't

5.3 Integration With Existing Systems

Below is a rich picture demonstrating the integration of the solution with other existing programs and stakeholders within the ecommerce landscape based on the current design. The diagram assumes that the company has an internal database of reviews to be displayed on the website and a database/application to store and manage support tickets. If either of these are missing the chatbot could easily be reprogrammed to capture reviews to a google sheet via a webhook and send support tickets as an email using a mail server however for the development of this product I will be using API stubs to represent the non existent external applications in my fictional ecommerce store. The rich picture also makes reference to the heavy lifting of some processes being handled by ChatGPT and the risks that come with using an external company in a time when AI regulations are a hot topic, with the OpenAI Chief recently calling for “an international body similar to the International Atomic Energy Agency to oversee rapidly advancing AI” at a conference in Dubai (Mirror 2024).

5.3.1 Rich Picture



5.4 Language/framework choice

Python & Flask

Python is renowned as the best language currently for all AI development due to the extensive number of libraries available to create LLMs and leverage OpenAI products. I also have experience with flask websites from several of my university modules and experience making LLMs from some volunteer work I did at JP Morgan during my placement

HTML & CSS
Used for creating the default website that the chatbot will be run against.

Bootstrap

Langchain
A python library that allows you to call ChatGPT with a reference document, allowing it to answer questions about any information in the document. This will be especially useful for customer support which relies heavily on the chatbot understanding the companies offerings, refund policies etc

5.4 Front End

100 Appendix

x.x Keyword Definitions (Move to appendix)

Term	Definition
Ecommerce specific	
Conversion	When a user buys the product intended by the seller
Software Engineering Specific	
LLM	Stands for Large Language Model and refers to a program that can recognise and generate text, commonly being trained on huge sets of data
Natural Language	Refers to most spoken languages, specifically the opposite of machine languages such as code
Other	
?	