Software Requirements Specification

Version 1.0

September 23, 2022

IT Helpdesk Portal

Parth Parmar

parthp1@umd.edu

Submitted in the partial fulfillment of the requirements of ENPM809W – Project Phase 1

Table of Contents

List of Figures

1.0 Introduction

1.1 Purpose

The purpose of this document is to present a detailed description of the IT Helpdesk Portal for a service provider. It will explain the purpose and features of the portal, dependencies and constraints of the project under which it is expected to operate, functionality and use cases for different stakeholders. In addition to the functional and non-functional requirements, this document will also highlight the security requirements and propose a threat model for the web application using STRIDE model.

1.2 Scope of the Project

This project will be a web application portal which will work as a platform for addressing the customers' queries with regards to the services of the company. This platform is designed in such a way that it will help not only the customers, but also the support team of the company to efficiently provide resolutions within a short time. This application will be used by both the company providing the service and its customers. Customers will be able to get solutions to all their problems through this portal and company will be able to effectively address customer issues and communicate common solutions to the customers by pointing to knowledge base articles. Thereby reducing the ticket resolution time and reduce the workload on support team.

More precisely, this portal is designed to allow a customer to track various issues within their account and request assistance on each issue. They will also have read access to articles for troubleshooting issues and comment on them. To access these services, customers have to login to the platform using their username and password.

1.3 Glossary

Term	Definition
Customer	A person who uses the portal for getting resolution to their concerns for the product in scope. They can view the knowledge base articles and raise tickets on the platform for support.
Database	Place to store all the data managed in this system
Portal	Web application which is used by all stakeholders for this application and access relevant services.
Customer Support Specialist	A person who looks after the case queue and responds to customer queries. They can also read and respond to knowledge base articles.
Administrator	A person who can view metrics about the system and create knowledge base articles for the

	customer seeing the type of queries often seen.
Ticket	A string which is used to identify a case.

1.4 References

IEEE. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.

1.5 Overview of Document

The next chapter, the Overall Description section, of this document gives an overview of the functionality of the product. It describes the informal requirements and is used to establish a context for the technical requirements specification in the next chapter.

The third chapter, Requirements Specification section, of this document is written primarily for the developers and describes in technical terms the details of the functionality of the product.

Both sections of the document describe the same software product in its entirety, but are intended for different audiences and thus use different language.

In the fourth and last chapter, Threat Modelling section, of this document is written for developers and testers. It helps in documenting various possible threats in the software system, their impact and security considerations which should be considered for mitigation.

2.0 Overall Description

2.0 System Environment

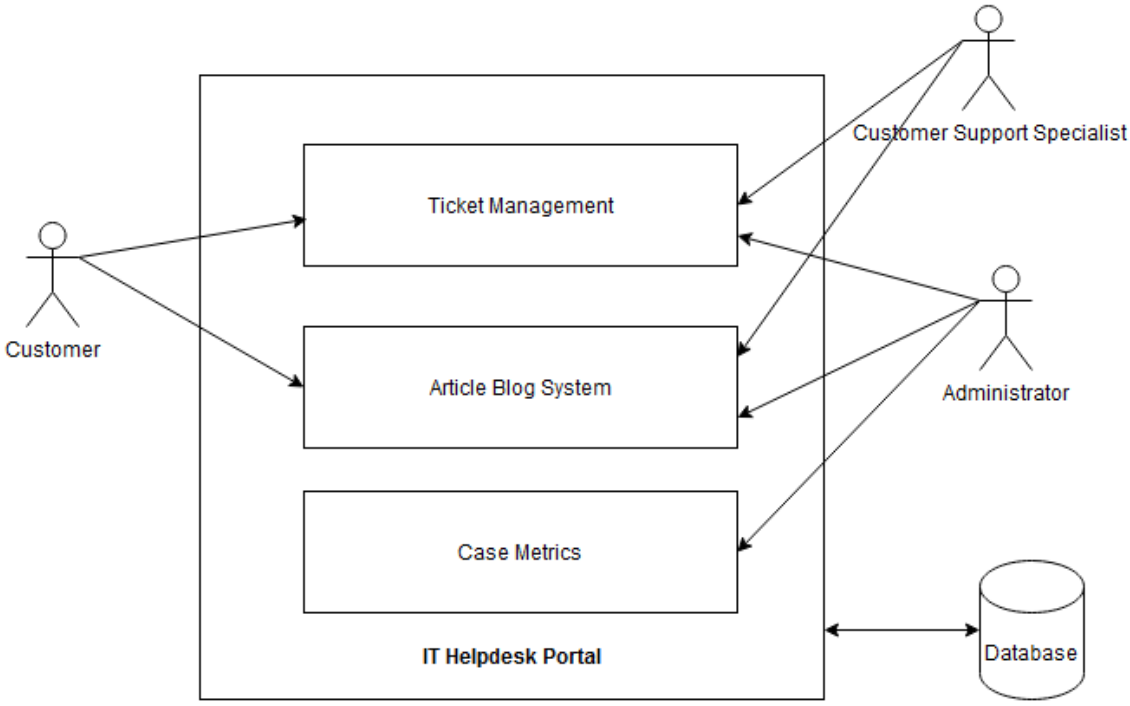


Figure 1 – System Environment

The IT Helpdesk Portal has 3 active actors and one software system. The Customer, Support Specialist and Administrator will access the portal through the internet, and each will have different access assigned to them. Depending on the requirements each actor will be exposed to certain extra functionality.

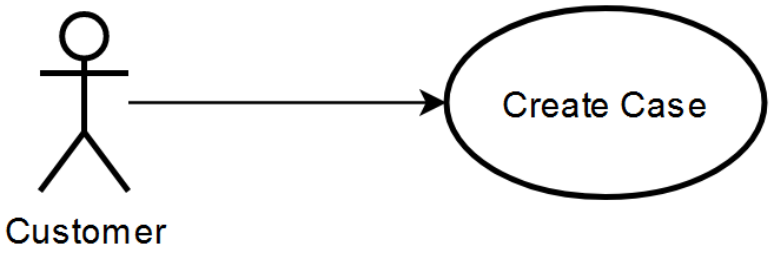
2.2 Functional Requirements Specification

This section explains the use cases for each of the actors separately. The Customer, Customer Support Specialist and the Administrator have some common use cases. While each one has a additional use case based on the role and the authorization.

2.2.1 Customer Use Case

Use Case: **Create Case**

Diagram:



Brief Description

The Customer access the portal, create a ticket for the resolution of the case and fill in the details for the query.

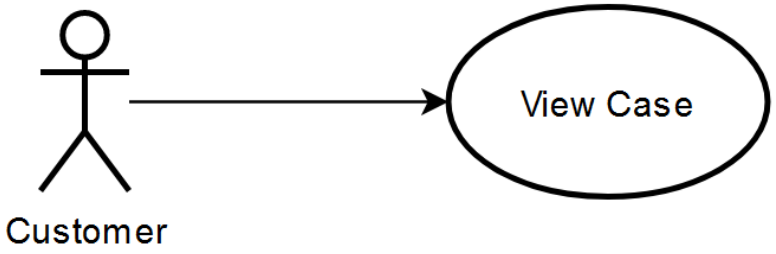
Initial Step-By-Step Description

Before this use case can be initiated, the Customer has already logged into the Helpdesk Portal.

1. The Customer clicks on the button for creating a case.
2. The portal presents various categories for the product selection.
3. The Customer selects a category from the list.
4. The portal asks for details from the customer for case creation including details like urgency, and short description.
5. The customer enters the relevant details and creates a ticket number for the query.

Use Case: **View Case**

Diagram:



Brief Description

The Customer access the portal, view old tickets which were submitted, are currently in review or closed due to resolution of the case.

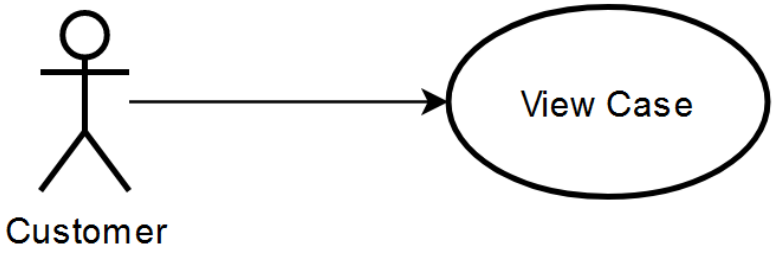
Initial Step-By-Step Description

Before this use case can be initiated, the Customer has already logged into the Helpdesk Portal and created a case.

1. The Customer clicks on the button for viewing a case.
2. The portal presents all the cases for that customer.
3. The Customer selects a case.
4. The system shows all the previous details for the case.

Use Case: **Close Case**

Diagram:



Brief Description

The Customer access the portal, close old tickets which are currently in review if they think they are satisfied with the resolution suggested by the support specialist of the case.

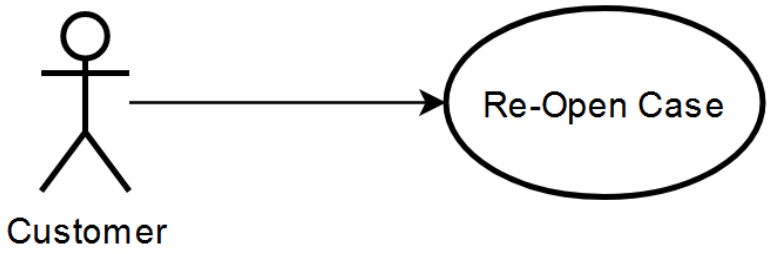
Initial Step-By-Step Description

Before this use case can be initiated, the Customer has already logged into the Helpdesk Portal and created a case.

1. The Customer clicks on the button for viewing a case.
2. The portal presents all the cases for that customer.
3. The Customer selects a case.
4. The system shows all the previous details for the on-going case.
5. The Customer can close the case if they are satisfied with the resolution.
6. Case is marked as closed.

Use Case: **Re-Open Case**

Diagram:



Brief Description

The Customer access the portal, view old tickets which were submitted and closed due to resolution of the case. And can re-open them when need be.

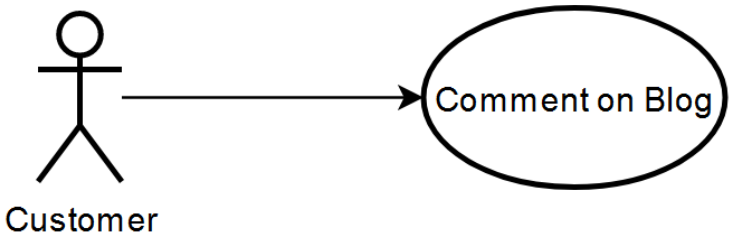
Initial Step-By-Step Description

Before this use case can be initiated, the Customer has already logged into the Helpdesk Portal and has a closed case in history.

1. The Customer clicks on the button for viewing a case.
2. The portal presents all the cases for that customer.
3. The Customer selects a case which is in closed state.
4. The system shows all the details for the closed case with an option of re-opening a case.
5. The case is re-opened and sent to the case queue for further review.

Use Case: **Comment on blog**

Diagram:



Brief Description

The Customer access the portal and view the blogs posted by the Administrator. Additionally, they can comment on the blog post if they have any questions or feedback.

Initial Step-By-Step Description

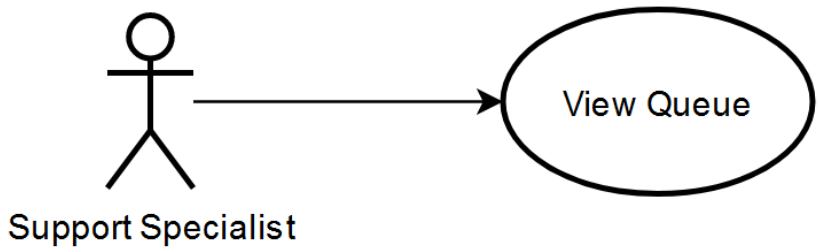
Before this use case can be initiated, the Customer has already logged into the Helpdesk Portal and the admin has uploaded at least one article in the blog system.

1. The Customer visits the blog page.
2. The portal presents all the blogs available in the system.
3. The Customer selects blog to read.
4. The system shows the contents of the blog and the comments made on that blog.
5. The customer can comment on the blog.
6. The blog will be updated with the added comment and displayed to Customer.

2.2.2 Support Specialist Use Case

Use Case: **View Queue**

Diagram:



Brief Description

The Support Specialist accesses the portal and is presented with available cases in currently in the queue.

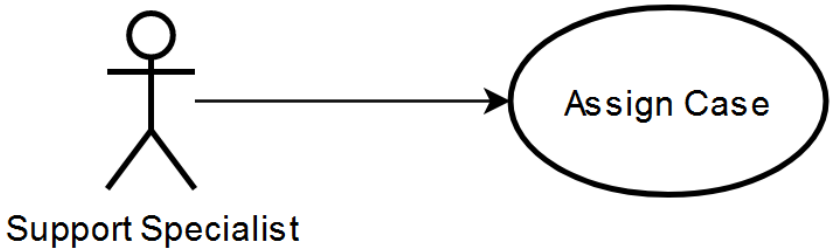
Initial Step-By-Step Description

Before this use case can be initiated, the support person has already logged into the Helpdesk Portal and there is at least one customer who has generated a ticket.

1. The Support Specialist views the case queue on the homepage by default.
2. The portal presents all the cases in the queue in a tabular form.

Use Case: **Assign Case/Work on Case**

Diagram:



Brief Description

The Support Specialist accesses the portal and is viewing cases on the main screen.

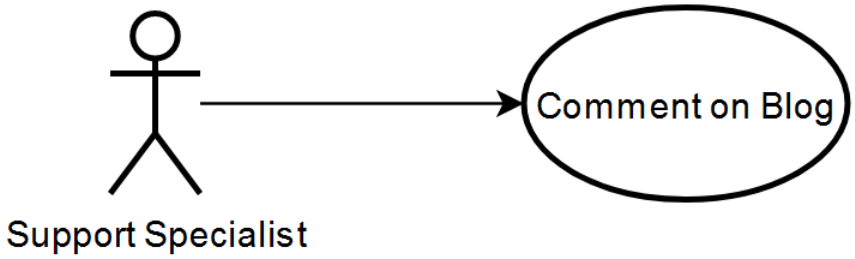
Initial Step-By-Step Description

Before this use case can be initiated, the support person has already logged into the Helpdesk Portal and there is at least one customer who has generated a ticket.

1. The Support Specialist views the case queue on the homepage.
2. The portal presents all the cases in the queue in a tabular form.
3. The Support Specialist selects one of the cases and assigns it to self.
4. The portal opens the case, and they can work on the case by replying to the customer.
5. All communications are updated on the case.

Use Case: **Comment on blog**

Diagram:



Brief Description

The Support Specialist access the portal and view the blogs posted by the Administrator. Additionally, they can comment on the blog post if they have any feedback on questions posted by customer.

Initial Step-By-Step Description

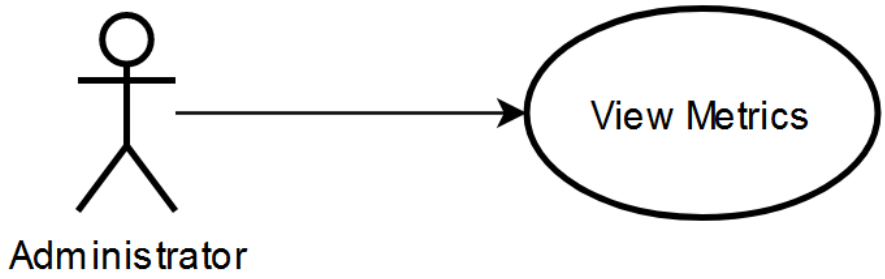
Before this use case can be initiated, the Support Specialist has already logged into the Helpdesk Portal and the admin has uploaded at least one article in the blog system.

1. The Support Specialist visits the blog page.
2. The portal presents all the blogs available in the system.
3. The Support Specialist selects blog to read.
4. The system shows the contents of the blog and the comments made on that blog.
5. The Support Specialist can comment on the blog.
6. The blog will be updated with the added comment and displayed.

2.2.3 Administrator Use Case

Use Case: **View Metrics**

Diagram:



Brief Description

The Administrator accesses the portal and view the case metrics by category of product.

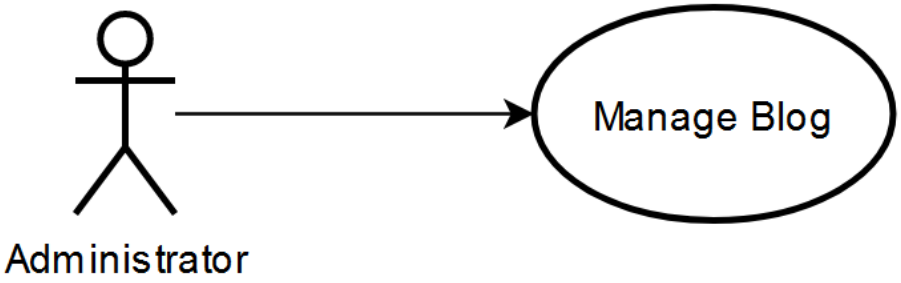
Initial Step-By-Step Description

Before this use case can be initiated, the Administrator has already logged into the Helpdesk Portal and there are at least 1 case resolved in each category to generate metrics.

1. The Administrator visits the home page.
2. The portal presents metrics available in the system.

Use Case: **Manage Blog**

Diagram:



Brief Description

The Administrator accesses the portal and can manage the blog in which admin can create blogs, edit blogs or delete blogs from the web application.

Initial Step-By-Step Description

Before this use case can be initiated, the Administrator has already logged into the Helpdesk Portal.

1. The Administrator visits the blog page.
2. The portal presents all published blogs available in the system.
3. The Administrator can select a blog post for editing or deleting the post.
4. The Administrator can also write a new blog for other users in the system.

2.3 User Characteristics

The Customer is assumed to be Internet Literate and be able to use a search engine. The main screen of the portal for customers will show the current open cases. They will have the option to view old cases and re-open them. Customer will also engage in reading blogs and writing comments on them.

The Customer Specialist is assumed to be Internet Literate and be able to use the portal for resolving queries. They will be the primary point of contact between the company and customer.

The Administrator is assumed to be Internet Literate and be able to use the portal and analyze the data from the metrics to create/edit/delete blogs in the portal.

2.4 Non-Functional Requirements

The IT Helpdesk Portal will be on a hosted on a local server in the company's premise and assigned a public IP. Customer's will have access to the server in the public domain using the public URL of the portal and credentials provided with the service.

The Portal here is assumed to be run on a server like ngnix or tomcat and uses https connection for the purpose of external communication between customers and the server. The latency will be based on the proximity of the user from the server.

The database will be a relational database like MySQL and hosted internally in a secure environment locally. All Clients accessing the portal will have installed a latest browser.

3.0 Requirements Specification

3.1 External Interface Requirements

There is only one external interface required which is Database running on premise of the IT company providing support service. This Database will help in managing the Customer data, track metrics and store blog information along with the comments specified in the portal.

3.2 Functional Requirements

3.2.1 Create Case

Use Case Name	Create Case
Trigger	The Customer or Support Specialist has logged into the portal.
Precondition	The page has an option to create a case in form of a button.
Basic Path	The Customer chooses to create a case based on the query they want to resolve. They click on the button on the homepage to create a new case. A form is presented with all the details to be uploaded. Optionally, a file upload functionality is presented. After the customer enters the category, they can enter all the case details. Submit the case details and generate a ticket ID.
Alternative Paths	In step 1, if the Customer wants they can ask the Support Specialist via other medium to create the case ticket. 1. The Support Specialist can create the case on behalf of the customer from within his portal. 2. Submit the details and generate ticket ID assigned to the customer.
Postcondition	A new case has been created in the database. Customer and Support Specialist's screen will be updated to show the newly added case. SLA time will start from the creation of the ticket.
Exception Paths	The Customer does not fill the details properly.

Other	The categories are filled from the Database.

3.2.2 Assign Case

Use Case Name	Assign Case
Trigger	The Customer or Support Specialist has logged into the portal and generated a case.
Precondition	There is at least one case in the queue.
Basic Path	1. Support Specialist
Alternative Paths	In step 1, if the Customer wants they can ask the Support Specialist via other medium to create the case ticket. 1. The Support Specialist can create the case on behalf of the customer from within his portal. 2. Submit the details and generate ticket ID assigned to the customer.
Postcondition	A new case has been created in the database. Customer and Support Specialist's screen will be updated to show the newly added case. SLA time will start from the creation of the ticket and registered in the database.
Exception Paths	The case is select by two support specialists at the same time. Then exception pops on one of the screens.
Other	The case is updated in the Database and timestamp is added.

3.2.3 Close Case

Use Case Name	Close Case
Trigger	The Customer or Support Specialist has logged into the portal. And the case is currently being worked upon.
Precondition	The page has an option to close a case in form of a button.
Basic Path	1. The Customer or Support Specialist chooses to close a case. 2. Either of the actors click on the close case button. 3. A dialog box asks the user about the reason for closing the ticket. 4. The user clicks on submit. 5. The case is closed.
Alternative Paths	N/A
Postcondition	The case has been marked as closed in the database. Customer and Support Specialist's screen will be updated to show the case in history/completed cases. SLA end time will be updated and the metric will be available to the Administrator's View.
Exception Paths	Both Customer and Support person closes the case at the same time.
Other	N/A

3.2.4 Re-Open Case

Use Case Name	Re-Open Case
Trigger	The Customer or Support Specialist has logged into the portal.
Precondition	The page has an option to re-open a case in form of a button. The case is already in closed state.
Basic Path	1. The Customer chooses to re-open a case based on the resolution given by the support group. 2. They click on the button on the case page to re-open a previous case.

	3. The state case is shifted from to active case. 4. Case is added to the queue for pick-up by a support person on the portal.
Alternative Paths	N/A
Postcondition	A state of case has been modified in the database. Customer and Support Specialist's screen will be updated to show the newly re-opened case. New SLA time will start from the creation of the ticket.
Exception Paths	N/A
Other	N/A

3.2.5 Comment on Blog

Use Case Name	Comment on blog
Trigger	Any actor is logged into the system and clicks on any blog's comment field.
Precondition	The page has an option to create a comment in form of a button with a text box above it.
Basic Path	1. The Customer chooses to view blogs by clicking on the blog tab on the screen. 2. Customer wishes to add a response to the blog for any questions. 3. They can enter the comment on the text box provided below the blog and click on submit to register the comment. 4. This will appear on the comment thread with the timestamp and the user who posted it.
Alternative Paths	Support Specialist can also do the above steps from their portal.
Postcondition	A new case has been created in the database.
Exception Paths	The blog will be updated with new comments. Database will be updated accordingly.
Other	All the people visiting after the comment has been registered will

	be able to see the comment.

3.2.6 Manage Blog

Use Case Name	Manage Blog
Trigger	The Administrator has logged into the portal.
Precondition	The page has an option to create a new blog. If there are previous blogs, then the Administrator can update/edit or delete the blog post using the portal.
Basic Path	1. The Administrator creates a new blog using the option. 2. They upload an html file which will be rendered in the blog page. 3. For editing the blog they have to upload the modified html file again using the "edit" functionality. 4. Optionally, they can set the authorization required to view the blog. By selecting, confidential, internal or public from the options.
Alternative Paths	In step 1, if the Administrator wants they can also delete the existing blog from the system. 1. The Administrator select the blog they want to delete and click on the delete button. 2. The data will be deleted from the data store of the database.
Postcondition	The blog view will be updated depending on the actions performed by administrator. If new one is added/edited it will be reflected in the blog view, else it will be removed from view in case of deletion.
Exception Paths	The Administrator upload empty file.
Other	N/A

3.3 Detailed Non-Functional Requirements

3.3.1 Logical Structure of the Data

The logical structure of the data to be stored in the internal Helpdesk Database is given below.

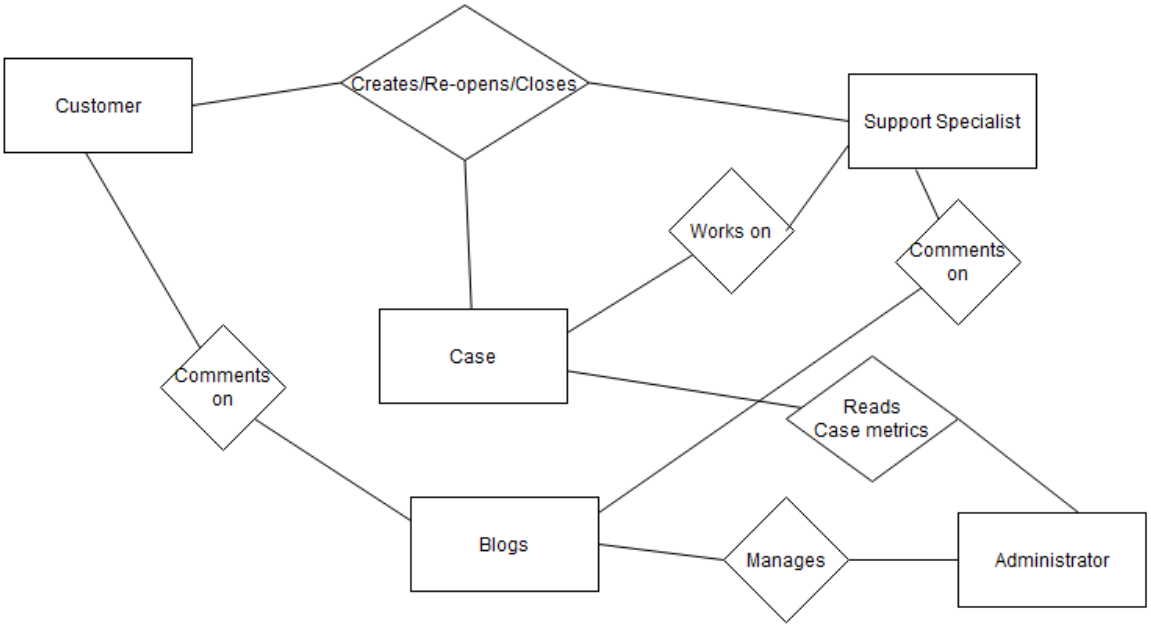


Figure 2 – Logical Structure of the IT Support Helpdesk Data

The data descriptions of each of these data entities is as follows:

Customer Data Entity

Data Item	Type	Description	Comment
Name	Text	Name of Customer	
CustomerID	Text	Uniquely Identify the customer	Primary Key
Email Address	Text	Email address	
Password	Text	Password of the Customer	Hash of the password

Support Specialist Data Entity

Data Item	Type	Description	Comment
Name	Text	Name of Support Specialist	

EmployeeID	Text	Unique identifier of the employee	Use to track the cases under the employee. (Primary Key)
Email Address	Text	Email address	
Password	Text	Password of the Employee	Hash of the password

Administrator Data Entity

Data Item	Type	Description	Comment
Name	Text	Name of Support Specialist	
Email Address	Text	Email address	
Password	Text	Password of the Employee	Hash of the password

Case Data Entity

Data Item	Type	Description	Comment
CaseId	Text	Uniquely Identify the case	Primary Key
CustomerID	Text	Uniquely Identify the customer	Foreign key
EmployeeID	Text	Unique identifier of the employee	Use to track the cases under the employee. (Foreign key)
ProductCategory	Text	Category of the product for the case	
Title	Text	Subject of the case	
Body	Text	Password of the Employee	Hash of the password
File Blob	Binary	File Binary	Optional
File Hash	TEXT	Hash of the binary	Optional

Blog Data Entity

Data Item	Type	Description	Comment
BlogID	Text	Uniquely Identify the blog	Primary Key
Access	Text	Access level of the blog	Can be public, internal or

			confidential
Title	Text	Subject of the blog	
File Blob	Text	HTML file	Required

3.3.2 Security

The whole application is on the company's premise. However, it is exposed to the public as well using a static public IP. Customers will be able to access the portal from public domain using the URL of the Helpdesk Portal. They will log in to the system using the credentials provided to them. They will only be able to access blog articles which are classified as public by the Administrator.

The Support team will access the portal internally within the intranet and access using their own credentials. They will be presented with many customer data which is stored securely in the database. They can only read the Blog articles which are tagged internal or public.

The Administrator will have a separate endpoint for the login not accessible by the Customers or the Support team. Admin can login and access the case metrics and view the blog which are classified as confidential, internal or public.

3.4 Misuse Cases

3.4.1 Misuse case: Modify case

Description:

If an attacker can access the account for support specialist or the customer, they can share information which may negatively affect the service intended by the web application.

3.4.2 Misuse case: Elevate privileges

Description:

An attacker can modify their role from customer, or support specialist to Administrator having access to all of the database and ability to modify blogs. Misinformation can be spread using the blog medium which can be harmful to the company.

3.4.3 Misuse case: Malicious Attachment

Description:

Customer or compromised customer account can create a case and submit a malicious file which if un-checked could be opened by the support specialist and compromise the whole intranet network.

3.4.4 Misuse case: Modify blog category

Description:

If an attacker has access to Administrator account, then they can essentially read all the confidential or internal articles meant for blog. This can lead to information disclosure.

3.4.5 Misuse case: Modify Case metrics

Description:

If an attacker can manipulate the case metrics generated from the database, they can benefit/harm from the numbers when administrator reads it.

3.4.6 Misuse case: Sniffing

Description:

As the customers access the data from the public facing server, the data could contain sensitive information. Hence the session should be encrypted to prevent from sniffing of data by an attacker.

4.0 Threat Identification & Modeling

Threat modeling activity helps the developer consider the various threats that could harm the smooth operations of concerned application. It helps document threats and classify them into a standard STRIDE model. So that developers can act on efficient mitigations around those threats. The Threat model specific to this application is shown as below:

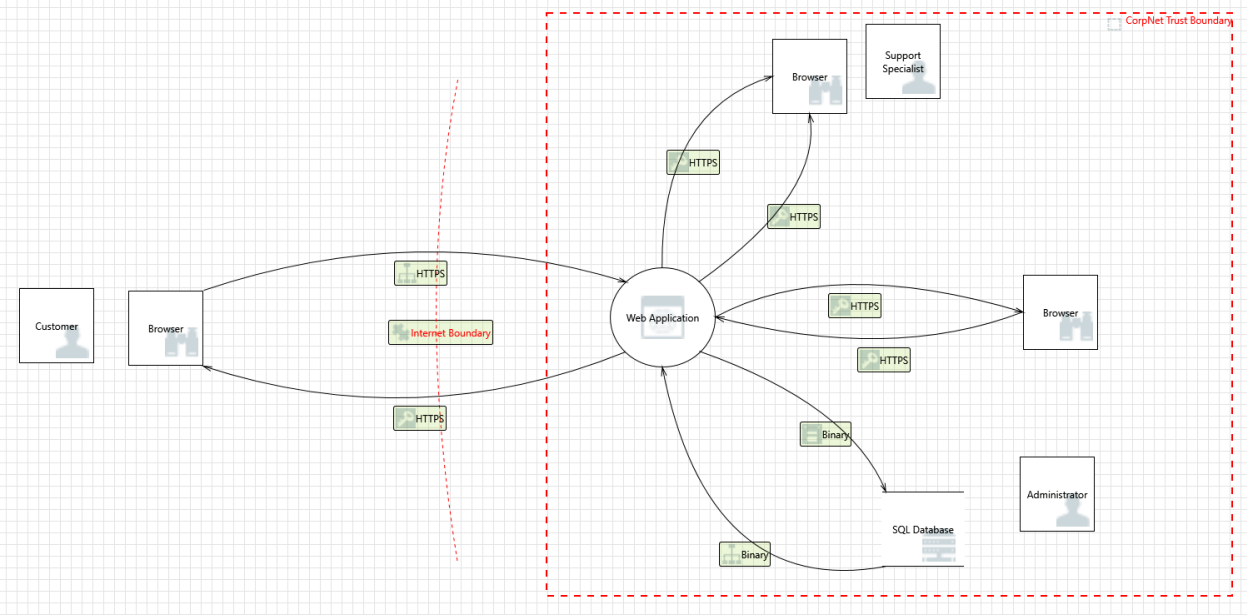


Figure 3: Threat Model for IT Helpdesk Portal

4.1 Threat: Malicious File Upload

Brief Description:

Malicious actor who has assumed role of customer or the customer can upload a malicious file which can cause denial of service in the web server or execute malicious code when opened by a support specialist. The execution of malicious binary could also allow the threat actor elevated privileges if executed in the intranet systems. Lateral movement is possible thereafter.

STRIDE - Denial of Service, Elevation of Privilege

Security Requirement:

The application inputs for file should be verified for file size and the type. Optionally they can be hashed to make a verification on external tools like virus total.

4.2 Threat: Customer Account Compromise

Brief Description:

If customer account gets compromised, then the spoofed actor can access case details that contain sensitive data it could be easily read leading to information disclosure or tampering the data of an on-going case.

STRIDE - Spoofing, Information Disclosure, Tampering

Security Requirement:

Session management data like cookies should be stored and transmitted securely. Use of CSP, HSTS and HTTP Only protections on client side should be implemented.

4.3 Threat: Support Account Compromise

Brief Description:

If Support Account gets compromised, then the spoofed person can access case details that contain sensitive customer data and read internal blogs leading to information disclosure or tampering the data of on-going case.

STRIDE - Spoofing, Information Disclosure, Tampering, Elevation of Privilege

Security Requirement:

Session management data like cookies should be stored and transmitted securely. Use of CSP, HSTS and HTTP Only protections on client side should be implemented.

4.4 Threat: Administrator Account Compromise

Brief Description:

If Administrator Account gets compromised, then the attacker can access all the data in database that contain sensitive customer data and read confidential/internal blogs leading to information disclosure or tampering the data of blogs in the portal.

STRIDE - Information Disclosure, Elevation of Privilege, Tampering

Security Requirement:

Session management data like cookies should be stored and transmitted securely. Use of CSP, HSTS and HTTP Only protections on client side should be implemented.

4.5 Threat: Malicious input

Brief Description:

The application involves various input fields everywhere. Those input fields could lead to client side and server-side attacks depending on the implementation. Every input should be validation to mitigate such types of attacks.

STRIDE - Information Disclosure, Spoofing

Security Requirements:

Every input should be properly sanitized before the application consumes it. Defense in depth methodology should be implemented and usage of not only publicly tested libraires but also custom manual validation on both server and client side should aid in reducing these types of threats.

4.6 Threat: Malicious Database Access

Brief Description:

Application interacts with database hence accepting input from application and safely converting them to SQL queries is essential. Otherwise, an attacker can manipulate SQL queries and have access to the database and maybe even modify it.

STRIDE - Tampering, Elevation of Privilege, Information Disclosure

Security Requirements:

Every SQL input should be parameterized and checked for malicious inputs by validating the inputs. Validation on every interaction from the application to the Database will help in mitigating the above-mentioned threat.