Data Security Health Map

Sponsor: Castle Ventures

Team Member:

Joel Ulahanna (PM)

Varun Shah

Aditya Gumastedesai

Viral Patel

Course Name: Masters Project CS700B-582

Instructor: Osama Eljabiri

Date: 12 December 2017

Table of Content

Chapter 1: Introduction

Let's start with a scenario. We want to protect our HR data. So, we create an Item Called HR data. We then should be able to say what makes up "HR Data". If we had a Visio like drawing screen we could drag and drop those components on to the "Map". We then could answer questions about each of the components along the scoring vector. We would enter those manually to get start for each of the components. Then we would aggregate them to come up with ta composite score of HR data. This is the easiest way to explain the data security health map application that will be explained in detail in this report.

1.1 Background

To understand why this application was create we need to know some background about the cyber-security industry. Castle ventures is the company that sponsored this project, is a cyber security consulting company. And this project is the brain child of the owner Mr. Arthur Hedge who is a graduate from MIT.

Business Need/Opportunity

Organizations continue to experience a record number of security breaches. A key contributor is that investment in security technologies is not targeted to critical data; instead 80% of spending is on defending infrastructure. This project will assist a company to improve its data security posture. It will allow an executive of a company to identify the company's critical data so that data security efforts can be focused on the most important information.

Product Description

- This application will provide companies with a platform to specify the details of critical data of the company. Details such as location of the data, the device and the drive in which data is stored.
- This detail will be recorded into database and these devices or drives will be monitored for any security breach or unauthorized access.

1.2 Objective

Business Objective

The goal of the project is to build an application that will make it easy for the company to identify and track its sensitive data so that the security team can protect it effectively.

Project Objective

- Design a front end which will take input from user the details of the critical data and send it to the database.
- Design and a maintain database to store information related to devices and drives that need to be monitored and devices that need to be excluded from being monitored.
- Develop backend functionality for server tracking and a method to scan for unmonitored sensitive data.

1.3 Project Scope

High level Requirements

- Locate actual critical data from the feedback received from the Interview form.
- Creating different database tables for
    - Device and drives that need to be monitored
    - To Store ways to monitor these devices
    - Devices that are currently being monitored
    - Devices that should be excluded from being monitored.

Tracking of the sensitive data at three levels, device, shares on that device, and files in a share.

Out of Scope

- Collecting security information from the monitored file servers, etc.
- There is no reporting module in this phase of the project.

Stakeholders

- Business Executives – The people who own the data will be able to specify what is valuable to them. They will also have a score as to how well their data is protected.
- Information Security team – The people who are responsible to protect the data will have the information they need to make sure they are focusing their efforts on the most important assets.

1.4 Approach:

Requirements: Each item can be measured along 1 to 10 vectors on a sale of 1 to 10. At any given time, an item does not have to have a score along all 10 vectors. Some may be "Not Measured Yet", "not relevant", or meaning we can get some measure of the security of an application without knowing the totality of the information about the application.

The product will operate from a top- down approach.

I can add an item such as an application and assign its scores manually for each of the 10 vectors. As I get further details I can replace the manual scores with calculated score from each of the components.

- Need the ability to bulk import devices.
- Need to integrate with active directory for user information. It would be helpful to have department information associate with each user so that scores could be tracked by department.
- Need the ability to replace owners in bulk.
- Different process for measuring and securing a data transmission.
- Need the ability to upload(Attach) documents to items. These could be Visio diagrams, CSV files, other items that people would use in managing and protecting data.
- Need to ability to export a score sheet for a selected set of ITEMS.

Item is the key table. An item can be a set, an abstract item, or a device. In certain cases, an item can "change" between these states.

Here are some operations that we need to support.

- An item can be created
- An item can be converted into a set
- An item can be converted into a device
- An item can be added to a set
- An item can be deleted
- An item can be retired
- An item can be renamed
- An item can have its attributes updated

An item can have its device “removed.” This would be if something about the device changed and we did not have any information about the new device. Th this case we would (V2- log the change that a device was retired) delete the device record from the device table and turn the Item Type from “Device” to “Abstract” Potential item types.

- Top level Item
- Abstract Component
- Concrete Component
- Abstract Device
- Concrete Device

Rule for deleting sets

- When you delete a set or item, never delete its underlying components unless the item is a device.

Item 1 to 1 with servers and other technical devices. Meaning every server should be in the item table. Each item in the Item Table could have a type such as:

- Item
- Company
- User
- Servers

Chapter 2: Project Management

2.1 Roles

We assigned role according to the strong suits and experience of each member,

- Joel Ulahanna – Project Manager & Software Developer
- Varun Shah – Software Developer (Middleware)
- Viral Patel – Software Developer (Database)
- Aditya Gumastedesai – Software Developer (FrontEnd)

2.2 Task Analysis

Task analysis is the process of learning about ordinary users by observing them in action to understand in detail how they perform their tasks and achieve their intended goals. Tasks analysis helps identify the tasks that your website and applications must support and can also help you refine or re-define your site's navigation or search by determining the appropriate content scope.

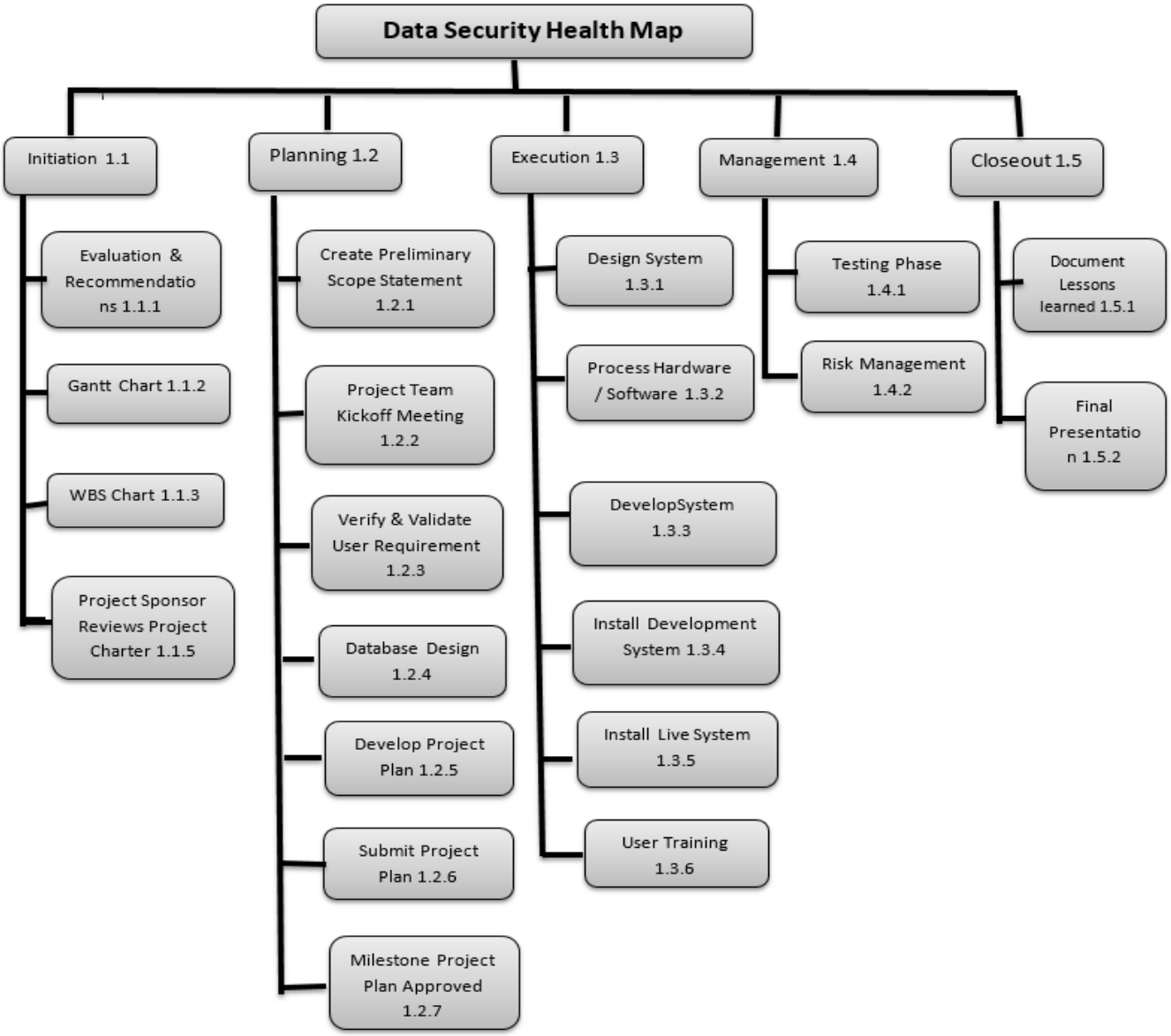
For the task analysis did we created the work breakdown structure which explains each part of the process of development of the Data Security Health Map. We also had the Office 365 Planner and the message portal called GroupMe for communication.

Details of the is mentioned in the further sections.

2.2.1 Work Breakdown Structure

a. **Initiation:**

   In the initiation process we will be focusing on creating and understanding the project that the sponsors need to be created and time line of the project. Here we will create the Gantt Chat and the WBS Chart as shown in the figure below



b. Planning:

Here we Make a note of the scope of the project. The requirements and the functions that was understood from the previous branch. We will go through a process of reviewing the document with the different stakeholders and plan how to approach the process and make the necessary changes to the time line.

c. Execution:

In the branch, we will design the system and Decide the hardware and software that will be used in the application. The details of this is mentioned further in this report. Here since we must execute the system, we will set the hardware servers and the software that are required. We create the application and set it up for live users to test.

d. Management:

At this process, we will start testing the application and asses the risk that the application may include.

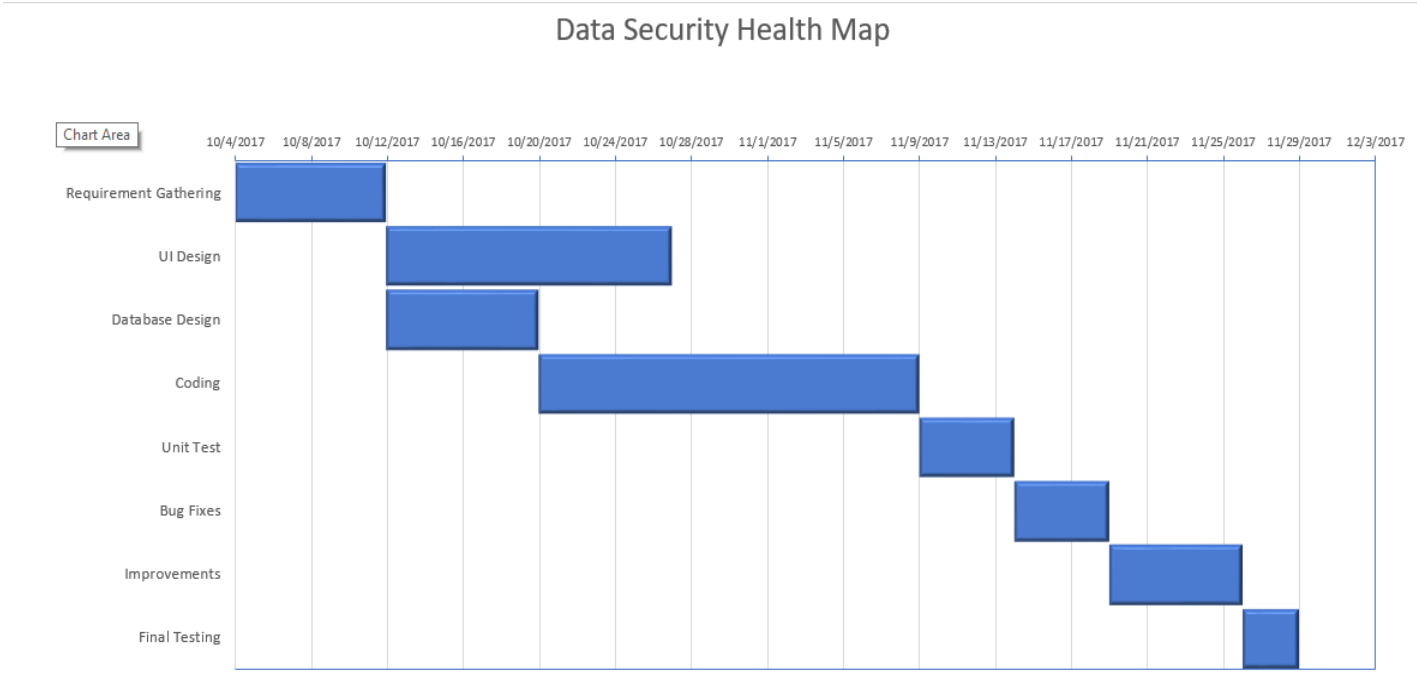
e. Closeout:

Here we document the application. The data that is required for other stakeholders to review and understand what has been accomplished in the duration of the development of this application.

2.2.2 Gantt Chart:

A chart in which a series of horizontal lines shows the amount of work done or production completed in certain periods of time in relation to the amount planned for those periods

The following diagram gives a general timeline of the development process.



2.3 Software Development life-cycle:

We used the agile process in the development of our project. We had daily scrums virtually. We used hangout to conference call every day at 8:30 AM in the morning to update each other on what our task for the day was. And in the evening at 6 PM we had left a message on the texting application that we used called GroupMe to inform the status of our task for that day. This process helped us stay motivated for the entire development process.

Every week we had one onsite meeting with the sponsors to show them our progress on the application. Sometimes they had some addition to the project. These details we discussed and a decision was made on how to incorporate it in our life cycle.

This agile process of development made us make progress with ease even if changes had to be made. If we had to pick another life cycle strategy we would keep breaking down because of the addition that we made by the sponsors, during the weekly meetings.

This process was ideal for the development of a web application. We would recommend this agile and Scrum method to any developer. It doesn't only work in a group process by also in individual application development process. This life cycle helped us complete our massive application with great easy.

2.4 Risk Identification:

The major risk that was identified was time management. This was due to the increasing scope of the project. Realizing that we had time constrains we had to curb the scope of our project to meet the deadline that we set.

The following table gives explain the risk analysis that was done for the Data Security Health Map application.

Risk Factor	Risk Statement	Likelihood	Impact	Level	Mitigation Strategy
Scope Risks					
Scope Creep	Lack of technical knowledge among team member to handle project due to unfamiliarity with language and application.	High	High	A	All team member must learn them together. The member with knowledge and experience can guide and teach other members of team.
TECHNICAL RISKS					
Lack of experience or expertise	A variety of framework and open source codes are available to aid us in project. However, we need to select the right tools to ensure security of website.	Low	High	B	To do an in depth research on the technologies used before start working on them. Also to do Proper documentation throughout the project for ease of change if the need arises.
Technological limitation	A variety of framework and open source codes are available to aid us in project. However, we need to select the right tools to ensure security of website.	Low	High	B	To do an in depth research on the technologies used before start working on them. Also to do Proper documentation throughout the project for ease of change if the need arises.
Project Management Risks					
Time Constraints	Even in the best planned schedule, unpredictable events are bound to happen. As a group of students who have different schedule and commitments, setting a common timeslot will be a challenge.	Medium	Medium	B	To have a proper planning of the project schedule: where, when, how and who to do tasks. All member must commit to a common timeslot to work on the project together. To also have buffer time for impromptu meetings for task completion in case of changes or unpredictable events.
Team Management	Conflict of opinions and working style.	Low	High	B	To establish team is harmonious yet efficient. To reverence and be open minded about the team member's view and working style. To make decisions as a team and resolve issues in a positive manner.

2.5 Project Management

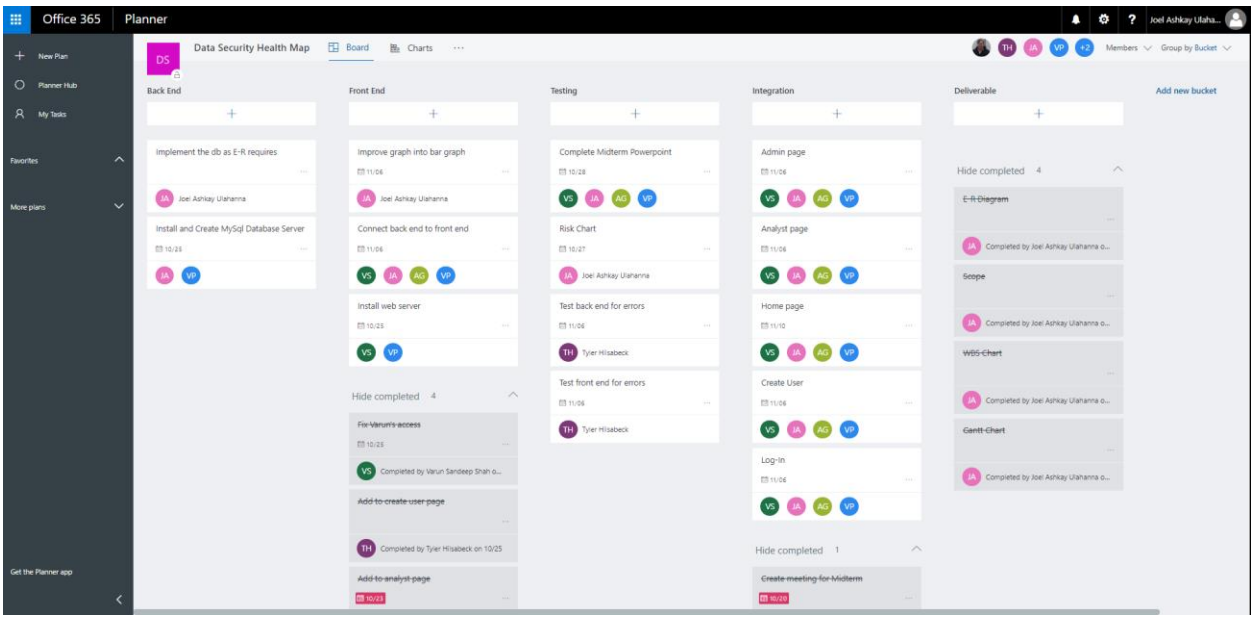
For the management of the development process of this application process we used different tools for different purpose.

Office 365 SharePoint:

For maintain a shared space of our data that we worked on we used SharePoint. We used this to maintain a record of all the document and application code updates. This made it easier for us to work remotely with great efficiency.

Office 365 Planner:

We used this tool to create a list of tasks that needed to be done and then assigned different members to different task. This application also gave us the benefit to assign a deadline for each task. This helps us to maintain a record of who oversees what task and if we were meeting our deadlines. This is a very helpful tool and we recommend it to other developers during their next application development.



2.5.1 Communication Management:

For efficient Communication, we had weekly meeting at the spencer's headquarters. For our daily communication and updates we use an application called GroupMe. This application helped us communicate daily doughs, issues faced and task completions effectively.

2.5.2 Human Resources:

As the PM of this project I had opened my doors to each member of my team. They can to me for issues in understanding the project and issues about working with each other's. I maintained a open communication with them related to any issues they had. I informed them to come to me with a problem that they faced dealing with the sponsors. This gave them the liberty to work without having to worry about expressing their feelings about anything. Overall there was open communication between every member of the project.

Chapter 3: Define

3.1 Stakeholder Analysis:

3.1.1 Internal Stakeholders:

1. Sponsors: Our Project 'Data Security Health Map' was sponsored by Castle Ventures Corporation. Tyler Hilsabeck was involved in the project planning and the requirement gathering stages along with the Project Manager and the Team Members. He also assured that project manager stayed on the tasks.
2. Project Manager: Our Project Manager Joel A Ulahanna was responsible for keeping track of completion of various deliverables of the project. He was also involved in the project development and planning phase. He positively influenced the team by helping us to stay on track by preparing progress report and submitting it on time.
3. Project Team: The Team was involved in development of the product. Each of the member was given a task and had to complete it in given time frame as per the planner. Team was also responsible for communicating with each other effectively and come up efficient strategies to implement the ideas.

3.1.2 External Stakeholders:

1. Business Executives: These are the clients who will be the end users of the product 'Data Security Health Map'. They are the people who own the Data and will be able to specify what is valuable to them. They will also have a score as to how well their data is protected.
2. Information security Team: These are the people who are responsible to protect the data time will have the information they need to make sure they are focusing their efforts on the most important assets.

3.1.3 Stake Holder Analysis Matrix:

Stakeholder	Impact	Influence	What is important to stakeholder	Contribution of stakeholder	Strategy for engaging stakeholder
sponsors	High	High	That the product is completed on time and working smoothly	Project Planning, Requirement gathering, Arranging meetings	Weekly Scrum meetings, discussions about new ideas and strategies
Project Manager	High	High	All the tasks are equally distributed among team members and making sure that development of product is on track.	Development of the product and Planning	Frequent communication and discussions.
Project Team	High	High	That the product is working correctly and all the requirements are met	Complete development and maintenance of the product	Assigning of tasks using Planner and Scrum meetings
Business Executives	High	High	Product helps to solve the company security related problems and make life easier	Providing with requirement	-
Information security Team	Medium	Medium	Product should be easy to use and user friendly so that they can make their analysis effectively	-	-

3.2 Project Scope:

This application will provide company with a platform to specify the details of critical data of the company. Company will also be able to specify the data that should be monitored and data that should be excluded from being from monitored. Based on the certain parameters of the critical data a graphical representation should be provided that gives the score of the security health of the data.

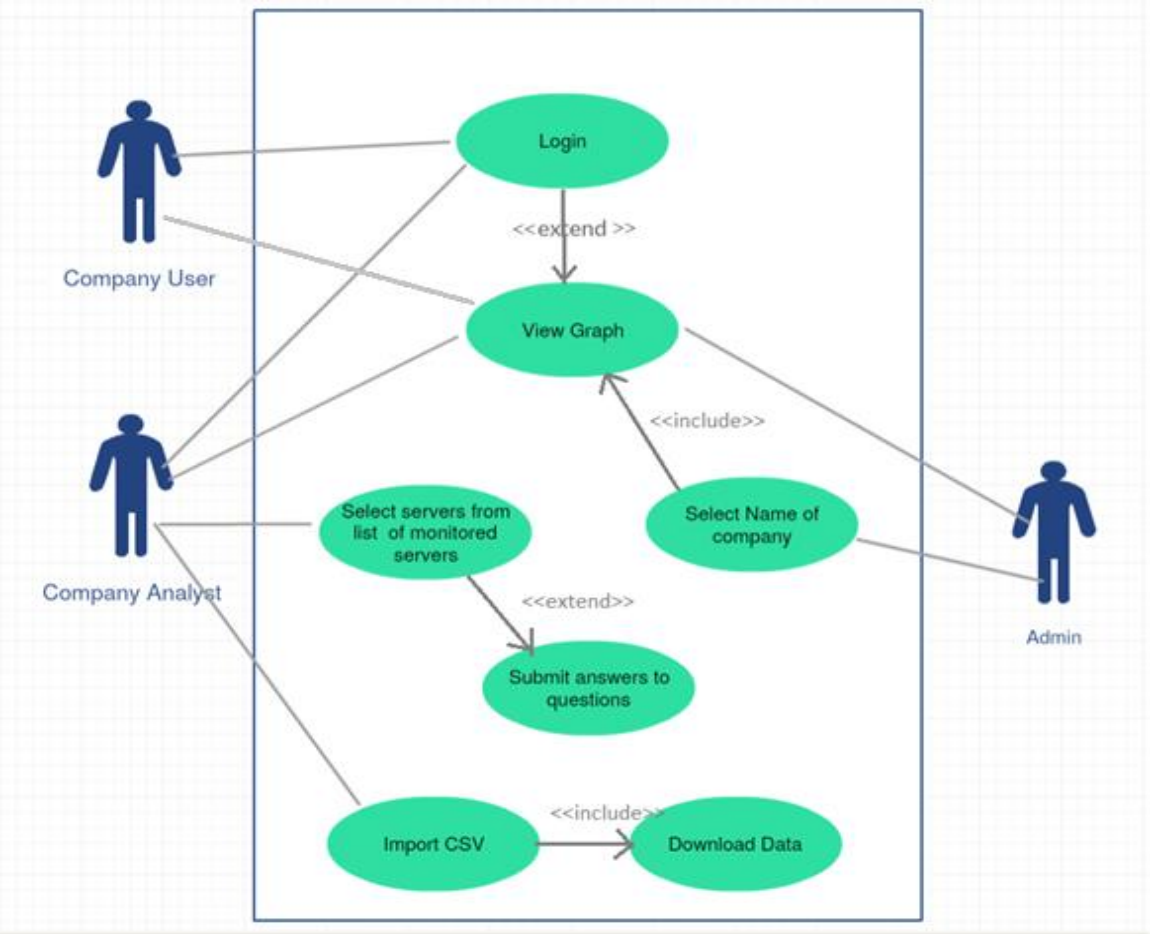
3.2.1 Functional requirements:

- System should implement authentication. Users should be able to log in and log out with correct set of username and password and view their profile.
- System should Implement import/export functionality that allows user to save data to database from CSV file or download data into CSV from the database.
- Analyst user should be given option to answers certain questions that will help generate the security health score.
- Accurate graph displaying security health score should be generated and displayed on the screen of the user.
- Admin user should have access to score of data of all the companies.

3.2.2 Non-Functional requirements:

- While implementing authentication the password should be encrypted and salted and saved to the database.
- Large CSV files should be imported and exported effectively and should not take large amount of time.
- Based on the type of the user, a user should receive proper privileges.
- Design a user-friendly Interface that should be easy to understand and operate for the users.
- System should be up and running 24 x 7.

3.3 AS-IS System and Use case:



Use Case Diagram

- There are 3 types of user
    - Company User: Company user will have access to only to the health score. He can view the graph that shows the security health score of the company data.
    - Company Analyst: Company Analyst can not only view the graph but is also responsible for answering certain question that will determine the security health of the company's data. Analyst user can also Import server's information to the Database using Import CSV functionality and then download the CSV containing all servers' information.
    - Admin: Admin User would be a user who has access to security scores of all the companies. Admin can also decide the weather what privileges to give to a user i.e. basic user privileges or Analyst privileges.

- Each user must login with his credentials to access his profile.
- After the Company Analyst logs in with his credentials, initially if there is o data for the company there will be no graph displayed. In this case the Analyst can import server information data into the Database using the import CSV functionality. He can specify which servers need to be monitored and which servers need to be excluded from being monitored into the CSV.
- After the Data is successfully imported analyst user can fill out answers to questions for each server that were uploaded using import CSV function.
- Once the user is done answering all the questions a security health score will be calculated and the user can view it on graph.
- Admin user can log in using his credentials and will have option to select any company and view its graph.

3.4 Requirement Gathering Technique:

3.4.1. Brainstorming:

- Brainstorming is an activity that is done in group and not individually.
- We used brainstorming techniques in the initial stage of the requirement gathering process.
- Time and place were decided for the meetings and we made sure everybody is on the same page regarding the idea of the product.
- Everyone was given a one objective to think upon for e.g. How the Admin page should look like.
- All the ideas from everyone were written down and best possible outcome was selected.

3.4.2. Prototyping:

- We used prototyping as another approach for requirement gathering.
- Different prototypes were created which contained online screens and feedback was taken.
- It helped in visualizing the app and getting a look and feel of how the workflow of the entire process is going to be.
- Different prototypes were created as the project progressed and requirements were modified accordingly.

3.4.3. Interviewing a stakeholder:

- This was one the three approaches that we used to clearly define the requirements of the projects.
- List of certain questions was prepared and were asked to the sponsors to gain clarity of the process.

- These questions included, who will be the users of the systems? what privileges should different users have? , what parameters should be considered while calculating a security health score? , What type of questions should be answered in order to generate the graph?

3.5 Project User Stories:

1. As a company user, I want access to view the security health map so that I can know the current security health of the company data.
2. As a company Analyst, I want access to view the security health map so that I can know the current security health of the company data.
3. As a company Analyst, I want to Import server information data to database so that I can answer questions related to security health of the server.
4. As a company Analyst, I want to download the CSV containing server information so that I know status of each servers.
5. As a company Analyst, I want to answer question related to security health for each server so that a graph displaying security health score can be generated.
6. As an Admin, I want access to security health scores of all company's data so that I can keep track of how secure every company's data is.

Chapter 4: Design

4.1 Study of Existing Solution to Problem

- Since to what extent we are seeing news where Sites, organizations has been affected with a digital assault or a risk from a programmer. It a very basic thing we are listening each day these sorts of news from everywhere throughout the World.
- For instance, starting from Uber to Equifax it's a standout amongst its most consuming issues of IT world. It's unrealistic to screen each server claimed by the organization at a same time.
- There's no such stage accessible to screen the health of sensitive information spread over all the server. Thus, the DSHM gives an interesting platform to end client, for example, security expert to see security as quantitative element.
- DSHM additionally gives the functionality of mass import-export of server comprising critical information and pick checking monitoring system for every individual server. What's more, to decide strength of specific server expert answers the quantitative inquiry with a specific end goal to decide graph for it.

4.2 Requirement of New System

- Because of issue and shortcoming in existing system, our proposed system gives the answer for every one of the issues in a solitary platform. DSHM is a platform accessible for all client to see the joined health of servers for respective organization. It likewise gives functionality to the analyst for exclusion when server doesn’t contain critical information to spare resources.

4.3 User Characteristics

User’s Role:

- User(basic) register him/her self along with personal detail and with company name. After that he/she will be able to log in to the system. This user is only able to see health graph for his/her respective company.

Company’s Role:

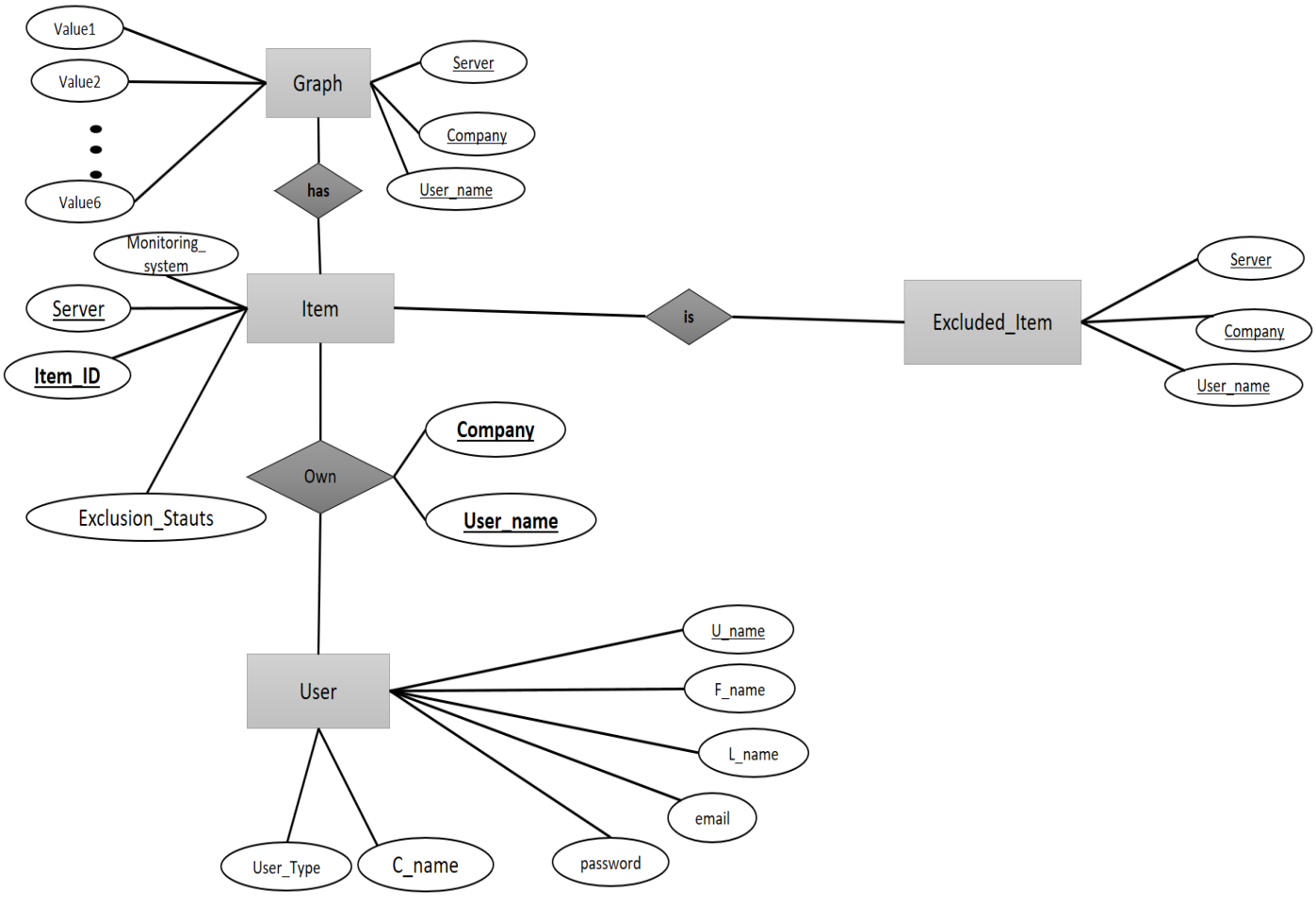
- Analyst (security person) act on behalf of the his/her respective company. Analyst is able to perform import of server company wants to be monitored and also import exclusion of server when it’s no longer priority.

- In the import functionality analyst mention server address, company and the monitoring system he wants for the server.
- Evaluation of the graph for server is also done by analyst. In which he/she answer the six-quantitative question for every server. The health graph for company will be evaluated by taking average of servers belongs to company.

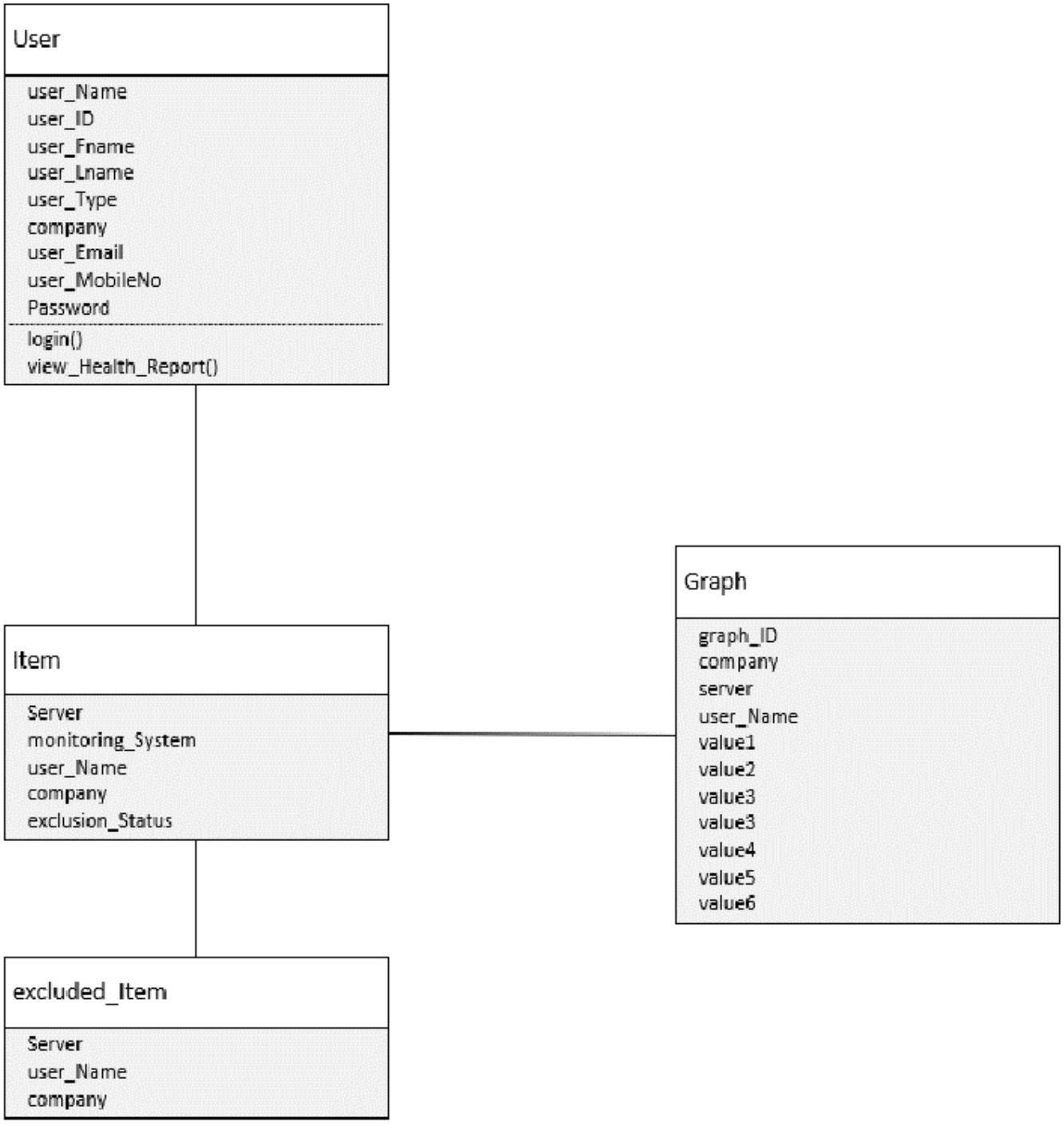
Admin's Role:

- Admin is the person of the Castle Venture company who's able to see the graph of every company registered in database. Admin can export the details of server being monitored and excluded from monitoring.

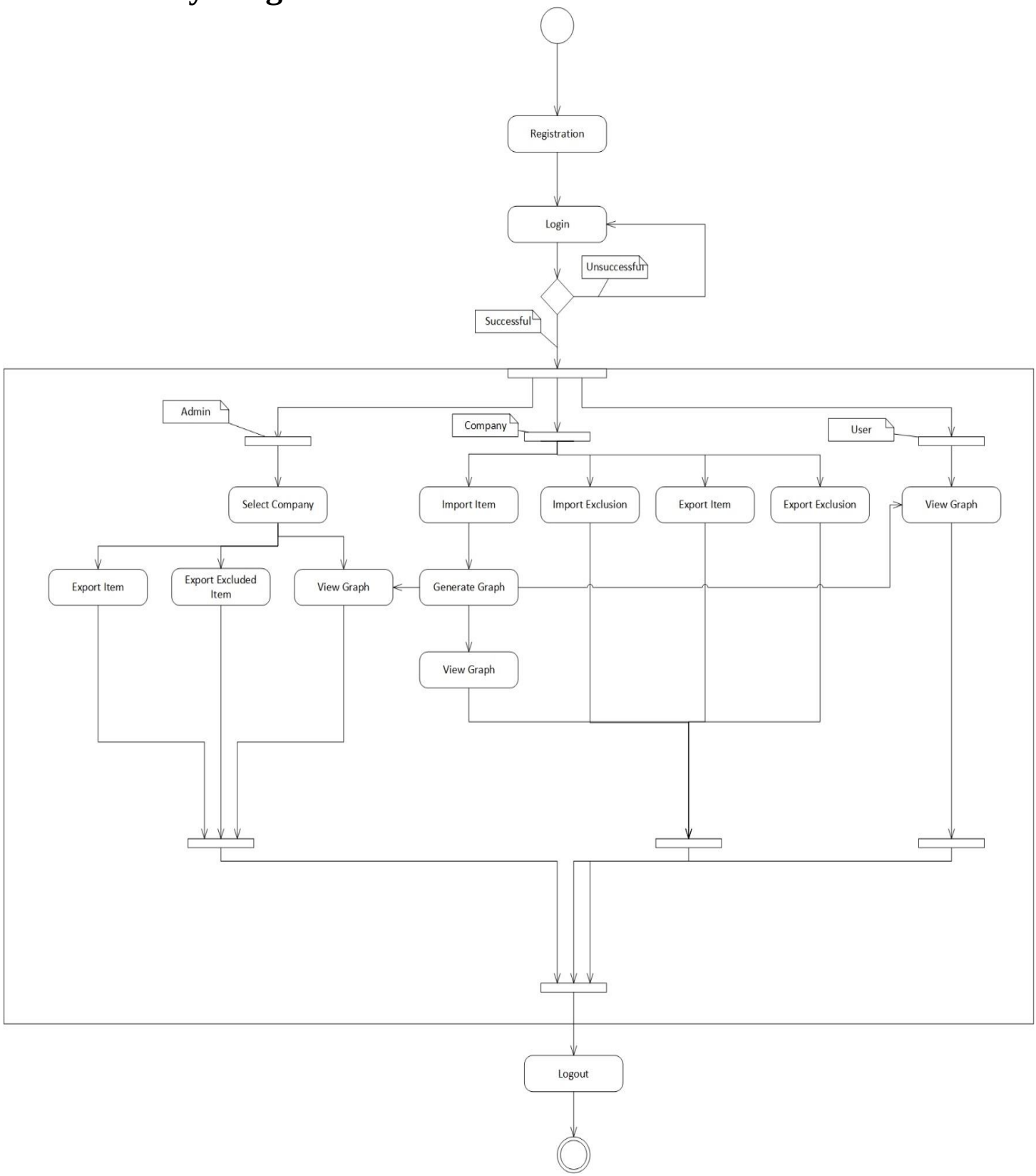
4.4 E-R Diagram



4.5 Class Diagram



4.6 Activity Diagram



4.7 Implementation

4.7.1 System Application Design

Method Pseudo Code

- Login
  a. Start
  b. [Login Page]
  UserName<-getParameter("UserID");
  Password <-getParameter("password");
  Company<- getParameter("company");
  c. [Check Usemame and Password and company]
  If UserName-username && Password=password && Company=company Then
  Redirect to homepage as per user_type;

  Else

  Write appropriate message;

  Goto Login Page;

  End if

  d. End

Import Item/Excluded Item

a. Start
b. [Import page]
c. Select excel file
d. Success Message
e. End

Export Item/Excluded Item

a. start
b. b.[Export page]
c. Save file
d. End

Evaluate Graph

a. Start
b. [Evaluation Page]
c. Select server
    i. Answer the six questions
d. submits

e. Success Message

View Graph

a. Start
b. [Search Company Page]
c. Select Company
d. View Graph
e. End

4.8 Database Design

- Database outlining is the way toward delivering, a definite information model of a database. This intelligent information contains all the required logical and physical outline decisions and physical stockpiling parameters expected to produce a plan in an information, definition dialect, which would then be able to be utilized to make a database. A completely credited information display contains. Detailed characteristics for every substance. While outlining the database schema, we have broken down various databases. Before beginning the framework, we have talked about with organization and worked likewise.
- The major objectives of the software design process are to document insufficient details of the software design based on the software requirements and traceability to specifications. All software design method shares the same goal to transform a set of data processing requirement into a computer program.
- Input design is a part of overall system design which requires attention very much. If an error occurs in the input data then the result of that error may lead to unwanted problems.
- The output is the most important direct source of information to the user. Intelligent output design will improve the system relationship with the user and helps in decision making.

4.9 Logical Description of Data

- The purpose of this section is to document a logical description of the data being collected. The intent is to provide a single integrated definition of the data that is unbiased toward any single application of the data being collected and is independent of how the data are physically stored or accessed. The intent is to provide a mutual understanding of the data being collected as well as provide a basis for systems database design and definition of the Physical Data Description. The logical data description is a data model, comprised of both a diagram and structured description (data dictionary) of the data objects, their relationships and their attributes. Although only the data dictionary is mandatory, it is strongly recommended that the graphical model also be developed to provide a complete logical description of the inventory data.

4.9.1 Database Table

Table Name	Description
User	Contains information about users of the system along with login detail
Item	Contains information about item(server), username, company name, monitoring system and exclusion status
Excluded_Item	Contains information about item(server), username and company
Graph	Contains the health result of each server evaluated by analyst.

4.9.2 Data Dictionary

4.9.2.1 Users

Field Name	Type	Constraints	Description
user_ID	Int	Not Null	Auto incremented and auto generated ID
user_Name	Varchar	Primary Key	It describes user name of an account
user_Fname	Varchar	Not Null	It describes first name of user
user_Lname	Varchar	Not Null	It describes last name of user
user_Type	Varchar	Not Null	It describes the user type of particular user
company	Varchar	Not Null	It describes the company name to whom user belongs
user_MobileNo_	Int	Not Null	It describes the mobile number of user
user_Email	Varchar	Not Null	It describes the email of user
user_password	Varchar	Not Null	It describes the password of user which will be stored

			after getting hashed and salted

4.9.2.2 Item

Field Name	Type	Constraints	Description
server	Varchar	Primary Key	It describes the address(IP) of server
user_Name	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and part of composite primary key
Company	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and part of composite primary key
monitoring_system	Varchar	Not Null	It describes the name of monitoring system for particular server
exclusion_status	Boolean	Not Null	It describes the exclusion of particular item form monitoring system which will be update by trigger set in excluded_item table

4.9.2.3 excluded_Item

Field Name	Type	Constraints	Description
server	Varchar	Primary Key	It describes the address(IP) of server
user_Name	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and part of composite primary key
Company	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and

			part of composite primary key

4.9.2.4 graph_value

Field Name	Type	Constraints	Description
graph_ID	Int	Not Null	Auto incremented and auto generated ID
server	Varchar	Foreign Key, Primary Key	It is the foreign key from item table and part of composite primary key
user_Name	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and part of composite primary key
Company	Varchar	Foreign Key, Primary Key	It is the foreign key from users table and part of composite primary key
Value1	Int	----------	It describes the the value for question 1 for respective server
Value2	Int	----------	It describes the the value for question 2 for respective server
Value3	Int	----------	It describes the the value for question 3 for respective server
Value4	Int	----------	It describes the the value for question 4 for respective server
Value5	Int	----------	It describes the the value for question 5 for respective server
Value6	Int	----------	It describes the the value for question 6 for respective server

Chapter 5: Development

5.1 Business Logic:

To prevent the systems from leaving any loose points. We have developed a system which takes in answers to sets of questions from the analyst of a company and these values help us determine the health score for that company. These health scores will help companies determine which servers are not monitored and which servers are being monitored, depending on this value of criticality of information can be determined.

The technologies used primarily consisted of:

- JavaScript
- Node.js
- SQL
- HTML5
- CSS3

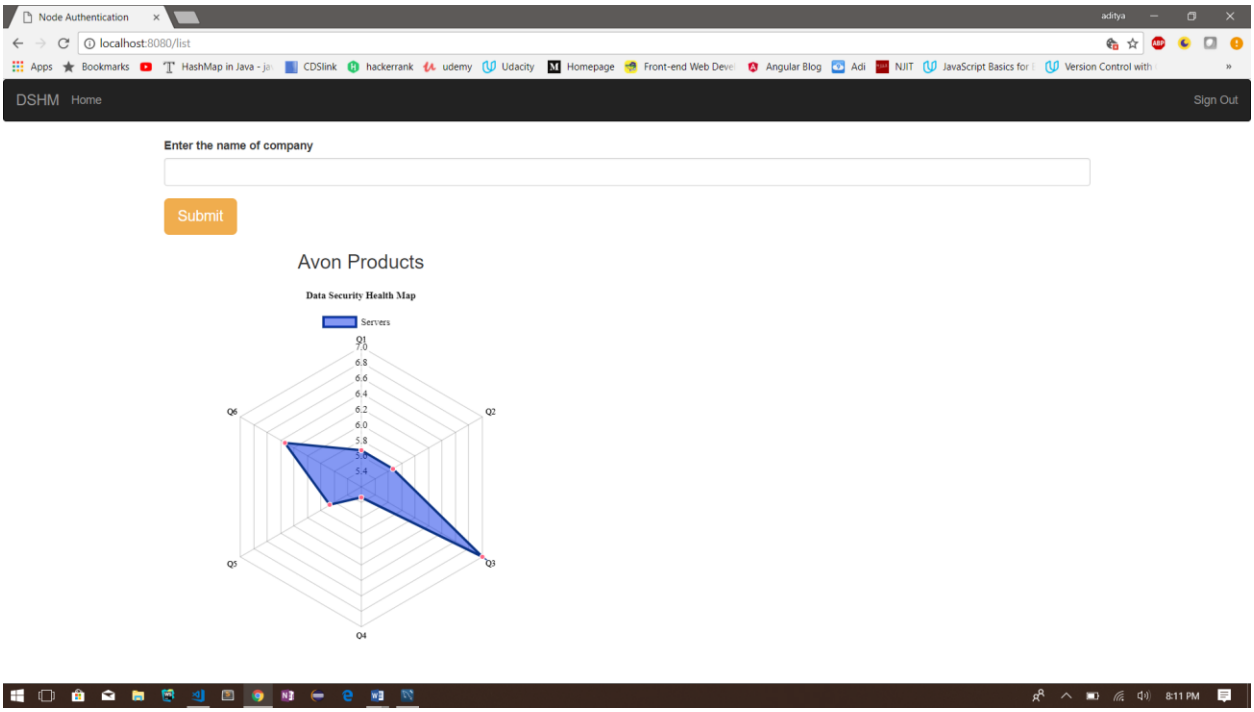


Figure: Admin page visible to only admin

5.2 Frontend:

Front end displays all the functionalities of the application to user. Interaction with user is recorded and stored in database. Powerful responsive frameworks like Bootstrap improves user's interaction with the machine. Front end allows users to take in input either through csv or through basic input and feed it into the database. Front end was designed using technologies like: HTML5, CSS3 and client JavaScript. Ejs (Embedded JavaScript) was the template used in front-end which helped us in displaying server side output to client interface. Logic behind integrating front-end to back-end was done using NodeJS.

Express library in NodeJS helped us in implementing RESTful routing like get and post request. Get request displays the content from server to client whereas POST request is used in writing contents to the server (ex: accepting user input field from registration page and giving to the server using POST request). These data is then sanitized by the server and then sent to database.

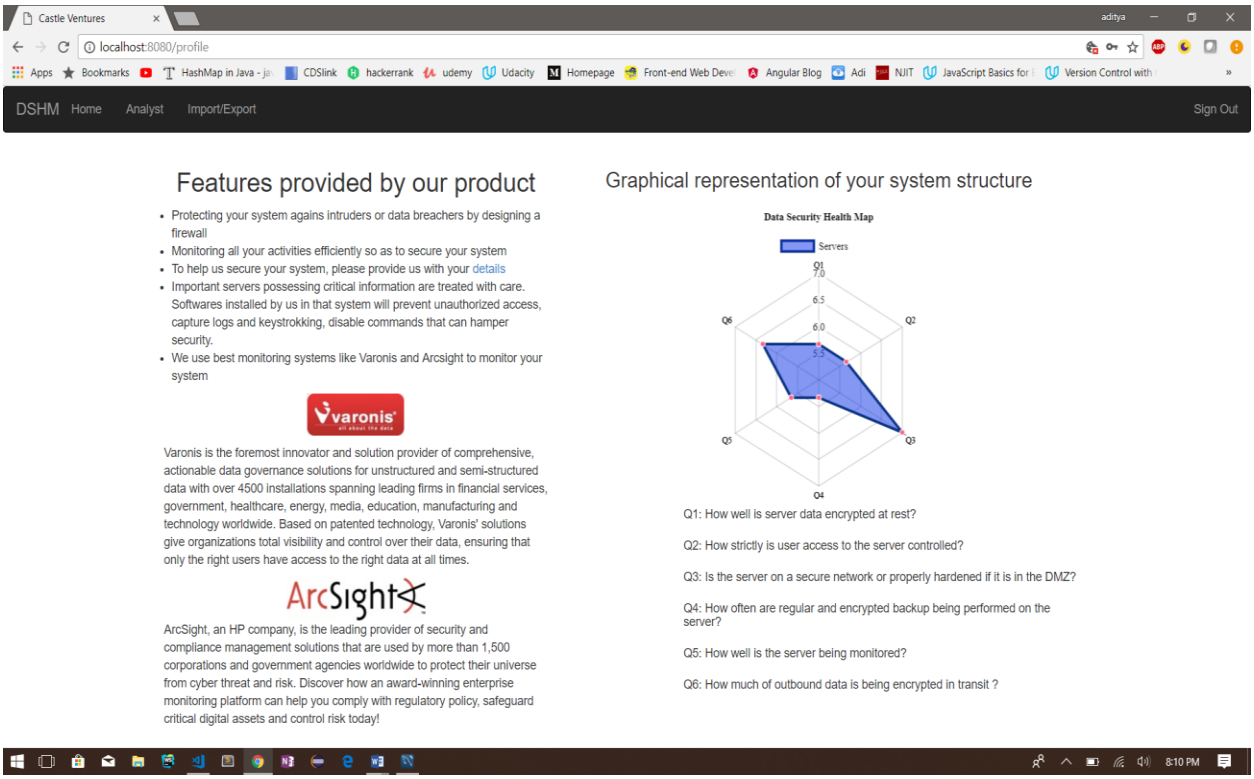


Figure: Home page visiblt to everyone after login.

There are 3 types of user in our system architecture: User, Analyst and Admin. Each set of users has different type of privileges like: User can only view the graph indicating health score of his company. Each set of users is distinguished by the id which he has these id helps distinguishing user and privileges. Analyst is the chief security head of the company. Analyst decides which sever should be monitored and which server should not be monitored. Analyst answers the questionnaire listed on the portal and based on the answer, a graph is computed which displays the health score of all his servers. Analyst can also exclude his server from being monitored by making a csv file having fields as name of server to be excluded. Admin will be the chief security staff of Castle Ventures company, admin can view graphs of any company. All he needs to do is provide the page with name of company, the server than communicates with database retrieves the value and provides those values to client, the client JavaScript uses these values to design Bezier curve and displays the curve to the admin.

5.3 Roadblocks and Challenges:

While making our project we ran into several roadblocks that arose to use of certain technologies and risks that were involved due to dependencies of getting from the other two teams.

- **Problems due to import server and import exclusion functionality:**
    - Import servers imported the data from user using csv file and imported these values to the database. The csv had 2 fields name of server and monitoring system. Only thing had to be done to achieve this functionality was extract the data from csv and insert it into the database using insert query. Problems started arising while importing exclusions. Import exclusions basically accept a csv file having servers as the field, based on the values to the field, the database will exclude the servers from the list such that in website those servers will not be shown, this task was very intricate as it involved updating database constraints and values based on values given by the users. A lot of research was done, this task needed all the resources from front-end as well as back-end. Eventually, we came up with the idea of triggers, whenever a file is imported, and if the values exists then a trigger will be fired which will update the values of servers from 0 to 1 indicating that servers needs to be excluded and should not be displayed in any website.

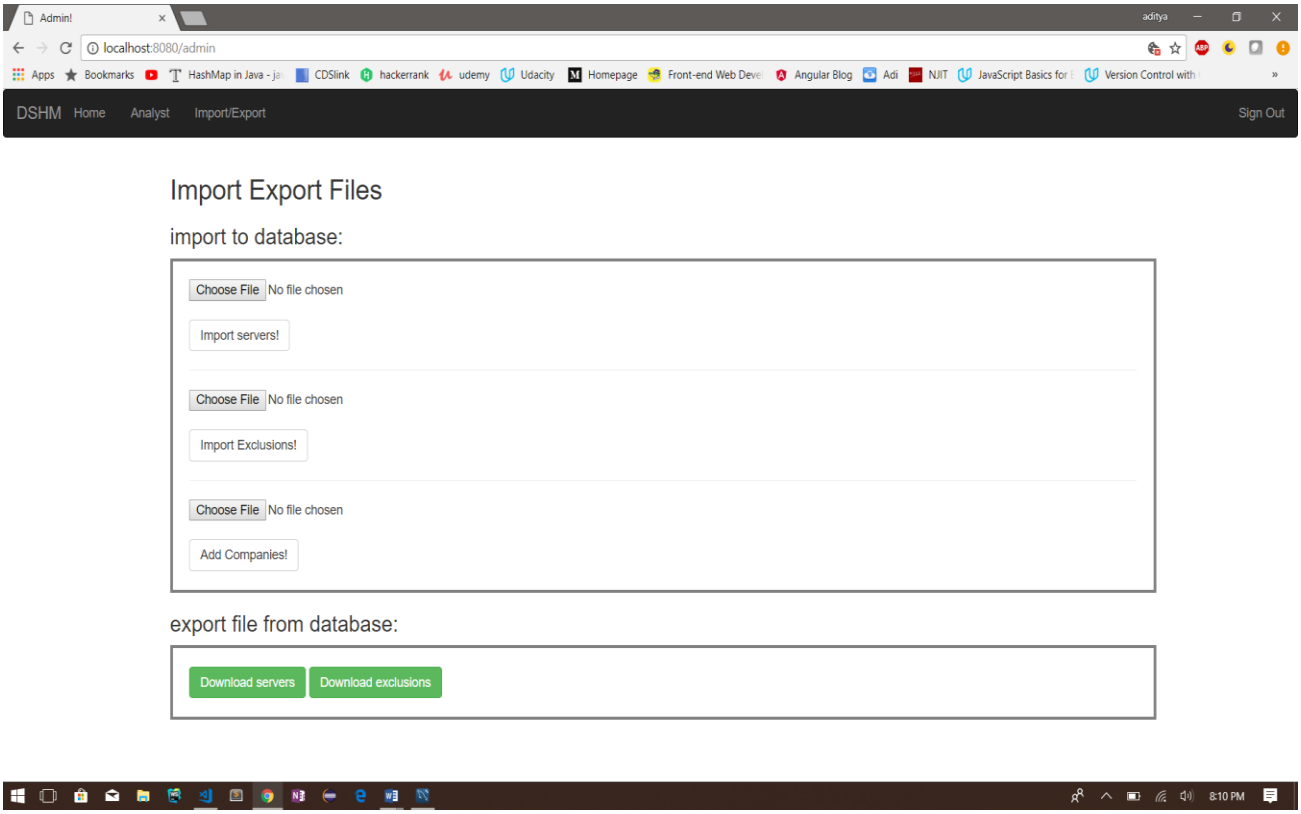


Figure: Import – Export functionality given by the analyst of users

- **Unavailability of list of questions:**
    - The graph designed was completely depended on list of questionnaires. Based on the answers to the questions, score is calculated. But without the answers, it was very difficult to create a graph as values to taken were unknown. This was a huge problem as main purpose for the application was graph without which, the main objective will not be fulfilled. Both front-end and back-end team relied on that questions. Later, a meeting was scheduled with stakeholders and in return were presented with 8 dummy questions. These dummy questions helped both front-end as well as back-end to design the team, this dummy values helped us design the graph in lucid and understandable way.

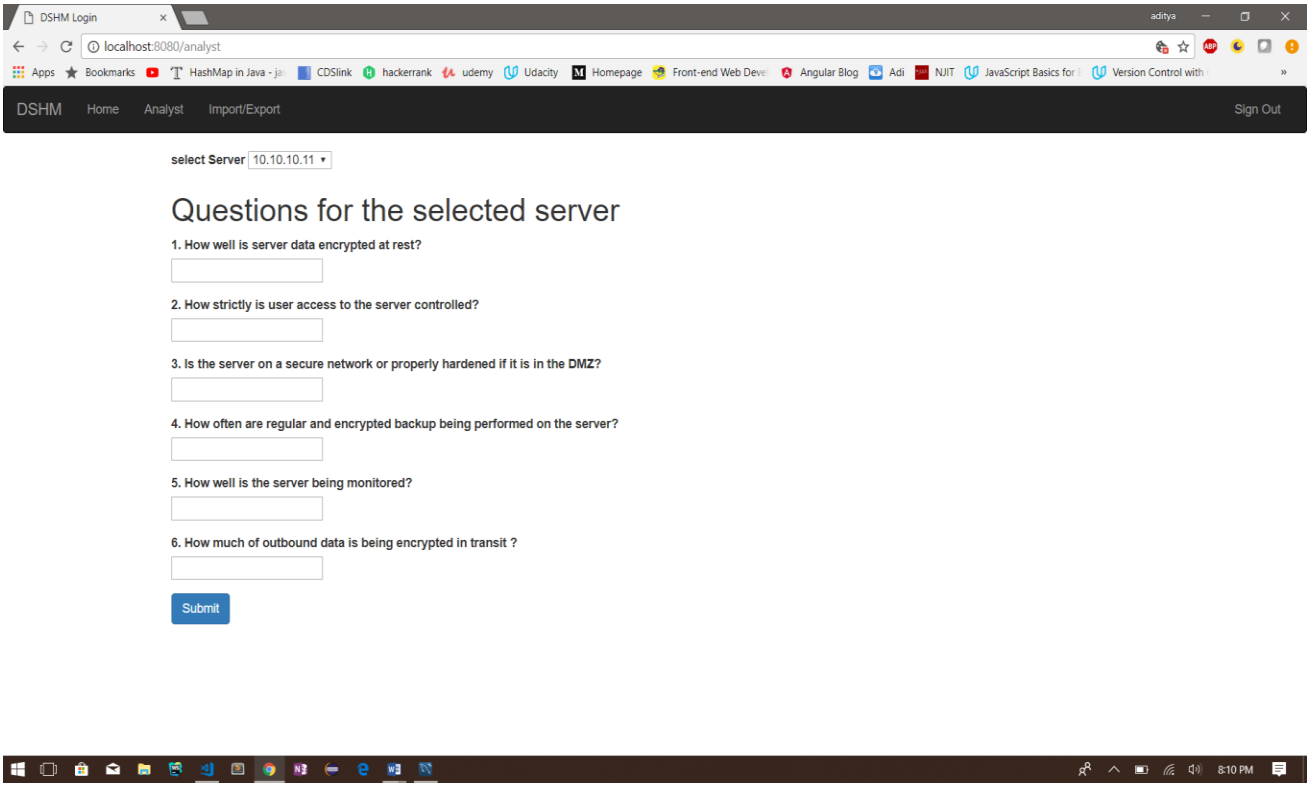


Figure: Questions received after having discussion with stakeholders.

Chapter 6: Evaluation and Conclusion

6.1 Solution Testing

Testing the solution created is necessary to assure product quality. This paragraph explains in detail the test planning, strategy and the methodology adopted to ensure that the solution developed is reliable and efficient.

Testing Scope:

- In Scope: Login, Input Fields selection, Verifying the result fetched from database, database connectivity, Performance of the solution when the data size is huge, Usability, Graph creation, Graph Display.
- Out of Scope: Stress testing.
- Items not tested: None.

Test Environment and Tools:

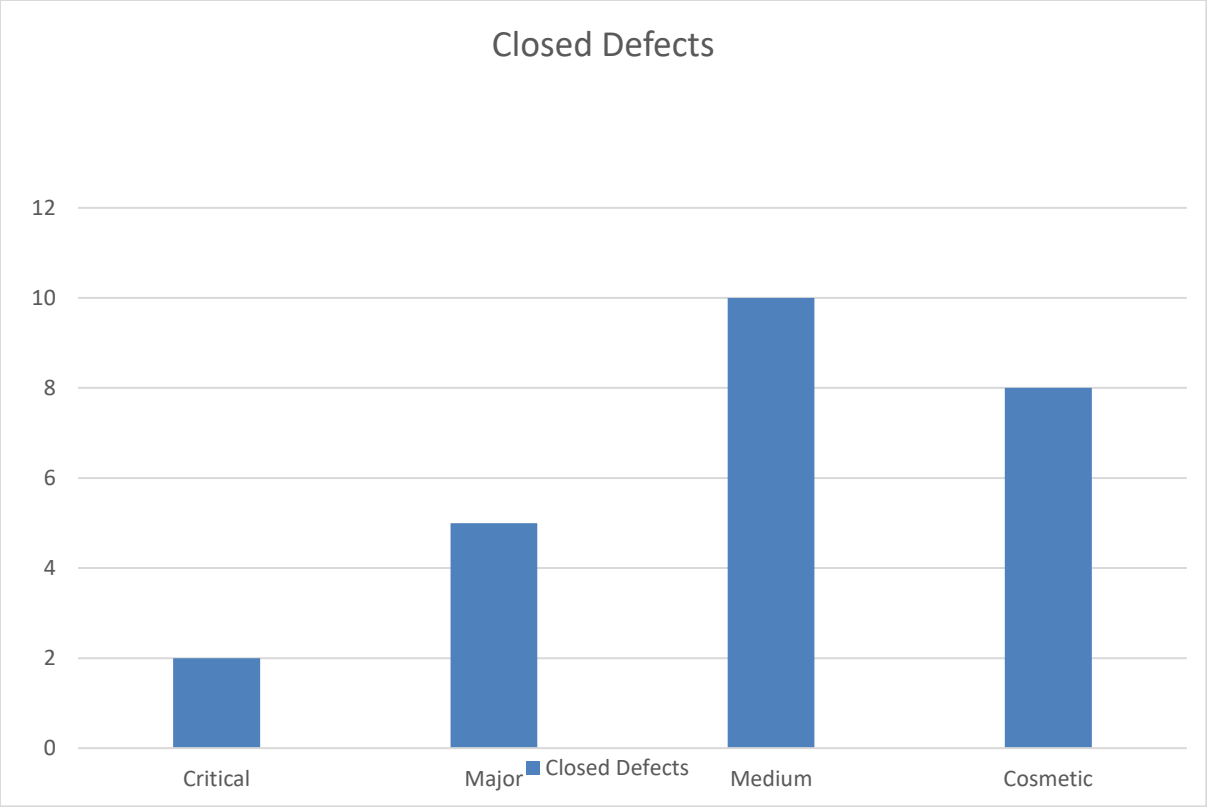
- Browser: Chrome, Firefox, edge.
- Database: MySQL
- Server: Linux Server supporting NodeJS

Final Metrics:

Test Case Planned	**Test Case Executed**	**Test Case passed**	**Test Case Failed**	**Coverage**
45	45	45	0	95.87%

Number of defects and their status and Severity:

	Critical	**Major**	**Medium**	**Cosmetic**	**Total**
Closed	2	5	10	8	25
Open	0	0	0	0	0



Types of testing Performed:

- Smoke Testing: To test the sanity of the build so that major functionality are working fine and to ensure that the build can be accepted for rigorous testing.
- Unit Testing: Performed by the developer when the new piece of code was developed to ensure the solution aligns with the requirements.
- System Integration Testing: Most of the application's data is fetched from the database. This type of testing was performed to ensure the connectivity to the database is accurate and the result fetched is appropriate.
- Regression Testing: After a defect was fixed this type of testing was conducted to ensure the change has not infused any new error into the system.
- Performance Testing: Large csv files were imported and exported to ensure the solution performs in a proper manner even when the data is massive.

Exit Criteria:

- All test cases should be executed – **Yes**
- All defects in Critical, Major, Medium severity should be verified and closed – **Yes**
- Solution is stable and reliable even when the data to be handled is huge.

Sign Off:

As the Exit criteria was met and satisfied testing was successfully completed and hereby signing it off for going live.

Defect Distribution:

	Log In	Search bar	Import/Export	Question Form	Graph
Critical			**1**		**1**
Major			**2**	**1**	**2**
Medium	**1**	**2**	**3**	**2**	**2**
Cosmetic	**2**	**2**	**1**	**2**	**1**
TOTAL	**3**	**4**	**7**	**5**	**6**

6.2 Quality Assurance

Quality Assurance is an integral part to determine if the solution developed as per the user requirement has undergone proper procedures and processes. It focuses more on the engineering process rather than engineering product. It helps in streamlining various activities involved in verifying the solution. It is being moreover process oriented. It can be described as preventive measure in ensuring the quality of the solution. It has basically three main aspects.

- Process definition and implementation
- Auditing
- Training

As a part of QA, we have taken care to align our code in a manner where all the developers follow a template. We also organized internal peer reviews for the code and as well as technical reviews so that the developed solution is optimized. Applying the test strategy gave yet another chance to ensure quality of the solution. Throughout the project we concentrated on adhering to the processes we set up in the start of the project.

6.3 Verification

Our system intended to map the health of all the servers for each company. Also, we had data for different company with had to be managed. Since this data was sensitive we had to see that we manage to maintain data integrity.

All these use case we successfully achieved to the satisfaction of our sponsors.

6.4 Team Conclusion:

What did we learn?

- The Importance of SCRUM to maintain coordination during the life cycle of the project.
- Maintain team relationships,
- Calculating the health of servers and managing them.
- New Programing language NodeJS and the use of bootstrap
- Database Management – we learnt how to manage a database to work efficiently and securely.

What would we do differently?

Even though our project went without any issues, we would have done one thing differently. The sponsors that supported our project we initially unclear about the requirement of the project. In the Future, we would make sure we had better details in the first meeting with our sponsors. This would make our project flow much smoother.

6.5 Critical Assessment

Though all the requirements and functionality of the Data Security Health Map were met there were few things that could have been done better in the application and in the life cycle of this project.

The 6 Security questions that were put forth we initially not quantifiable which was later converted into quantifiable values. Yet this would officially not satisfy every customer. Having a one analyst give certain values to a server seem to be too risky. I think if given more time we could come up with a better solution to solve this issue.

6.6 Version 2.0

For every application to be successful we need to know the weakness of our application. Here are some thoughts on the version 2.0 of the DSHM. Firstly, the issue of the question vectors that are used to quantify the health of the application must be solved

Our version 2.0 would have the following features:

- Include information about threats and threat analysis
- Ability to generate report from the system.
- Ability to include remediation tips based upon weaknesses that are identified.

Bibliography

- Task Analysis: https://www.usability.gov/how-to-and-tools/methods/task-analysis.html
- Test Matrix: https://www.guru99.com/how-test-reports-predict-the-success-of-your-testing-project.html
- Samples: http://searchsoftwarequality.techtarget.com/tip/How-to-write-an-effective-test-report