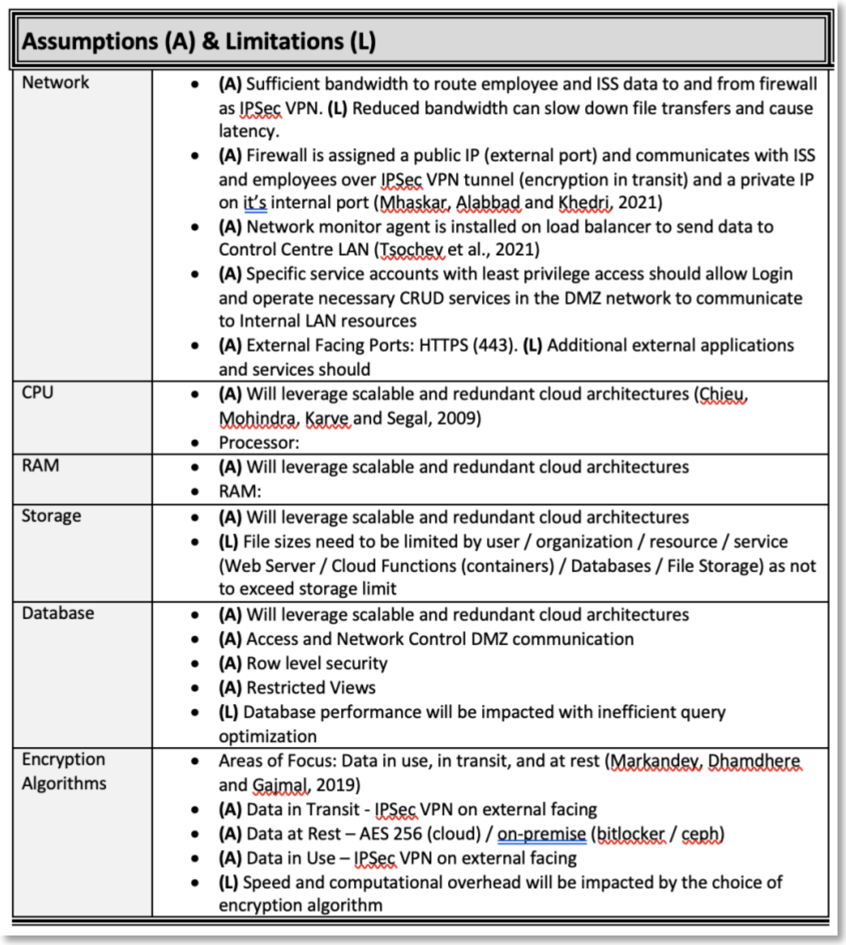
Our team was tasked to design and develop a secure file repository for NASA's ISS Safety Task Force using open-source libraries, leveraging development frameworks and system/software security technical controls in mind. The platform will allow NASA to collaborate with international partners via the secure repository. The team created a design document, highlighting the purpose of the application, system requirements/limitations/assumptions, tools and libraries, CIA (confidentiality, integrity, and availability) security controls, STRIDE modelling, and UML diagrams.

Our team lacked programming skills which was one of our biggest challenges throughout this module. The module name alone (Secure Software Development) gave me anxiety because I knew how difficult it was to complete another programming assignment from my first module. Although I possess the necessary knowledge for secure system design and secure software development, it didn't help with developing. I used that knowledge for the first part of this module (Unit 3) to create the limitations and assumptions doc (**FIGURE 1**) and review the work done by my team. With our experience combined, we were confident with our design document, ensuring we covered all security controls applicable to our application. However, due to the lack of our programming knowledge, translating the design to code posed a big challenge for us. We understood what needed to be in place for a secure web application but didn't have the real-world experience to develop it. In the real-world, going against our design document would have affected our timeline which would make the client unhappy, most probably leading to contract termination or at a least a change request.



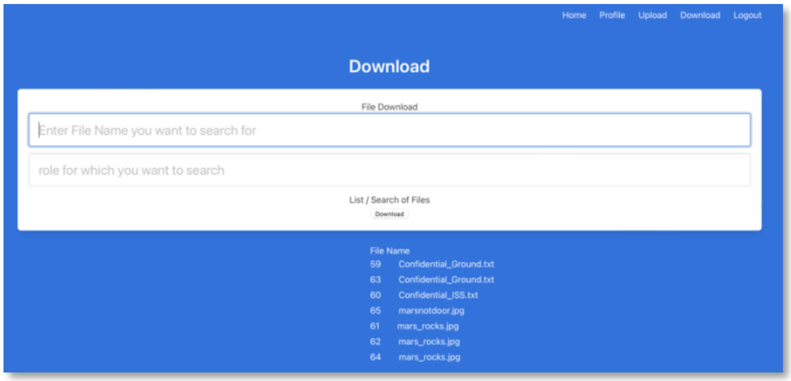
Assumptions (A) & Limitations (L)	
Network	• **(A)** Sufficient bandwidth to route employee and ISS data to and from firewall as IPSec VPN. **(L)** Reduced bandwidth can slow down file transfers and cause latency. • **(A)** Firewall is assigned a public IP (external port) and communicates with ISS and employees over IPSec VPN tunnel (encryption in transit) and a private IP on it's internal port (Mhaskar, Alabbad and Khedri, 2021) • **(A)** Network monitor agent is installed on load balancer to send data to Control Centre LAN (Tsochev et al., 2021) • **(A)** Specific service accounts with least privilege access should allow Login and operate necessary CRUD services in the DMZ network to communicate to Internal LAN resources • **(A)** External Facing Ports: HTTPS (443). **(L)** Additional external applications and services should
CPU	• **(A)** Will leverage scalable and redundant cloud architectures (Chieu, Mohindra, Karve and Segal, 2009) • Processor:
RAM	• **(A)** Will leverage scalable and redundant cloud architectures • RAM:
Storage	• **(A)** Will leverage scalable and redundant cloud architectures • **(L)** File sizes need to be limited by user / organization / resource / service (Web Server / Cloud Functions (containers) / Databases / File Storage) as not to exceed storage limit
Database	• **(A)** Will leverage scalable and redundant cloud architectures • **(A)** Access and Network Control DMZ communication • **(A)** Row level security • **(A)** Restricted Views • **(L)** Database performance will be impacted with inefficient query optimization
Encryption Algorithms	• Areas of Focus: Data in use, in transit, and at rest (Markandey, Dhamdhere and Gajmal, 2019) • **(A)** Data in Transit - IPSec VPN on external facing • **(A)** Data at Rest – AES 256 (cloud) / on-premise (bitlocker / ceph) • **(A)** Data in Use – IPSec VPN on external facing • **(L)** Speed and computational overhead will be impacted by the choice of encryption algorithm

FIGURE 1 – Assumptions and Limitations

This project presented a huge learning curve for the team as all our experience and knowledge within the information technology realm was outside of development. We created a list of features necessary for the application and prioritized them as a team – must have, should have, and nice to have. Once prioritized, we created tasks and sub-tasks in Monday Workspace, a project management SaaS. We divided up the tasks and got to work.

I was tasked with developing the logging function, search function, and list function. Additionally, all members of the team were responsible for app functionality testing and adding onto the ReadMe document. I was overwhelmed from the start because I was unable to attend the first couple of group meetings due to time zone differences. I reviewed the meeting recordings but was still behind with my features. I began working on my features later realizing someone had begun part of the work for it, like creating the necessary files to complete their features. This didn't help me when trying to commit my code to the main branch in our github, getting numerous merge errors. Without attending the meetings and syncing up with my group, I ended up doing a lot of duplicate work which later I found out was partly completed. The time I spent learning how to write the functions and add them to the existing code felt like a waste.

Another issue was that only one group member had access to approve code commits. So, if something wasn't working locally on their computer, it wouldn't get approved, although it would be working locally on mine. For example, our listing and search functions were working on my computer (**FIGURE 2 and FIGURE 3**) but didn't work on our group member's computer forcing him not to commit it in time for our presentation. It was disheartening to not see my code be part of the final project but I'm proud of my persistence to learn how to create the function and actually write the code.


Home
Profile
Upload
Download
Logout
Enter File Name you want to search for
role for which you want to search
Download

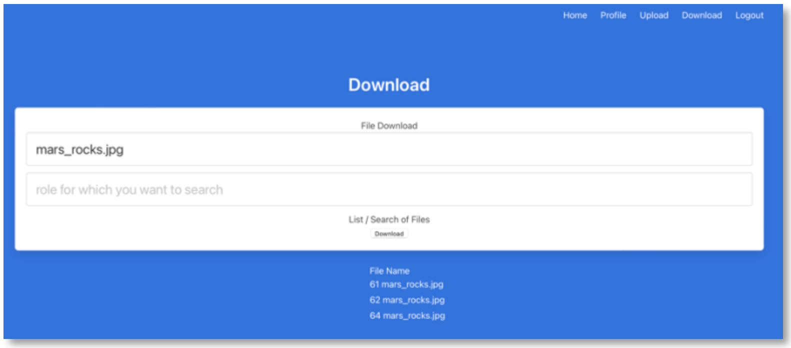
Download

File Download

List / Search of Files

```
File Name
59      Confidential_Ground.txt
63      Confidential_Ground.txt
60      Confidential_ISS.txt
65      marsnotdoor.jpg
61      mars_rocks.jpg
62      mars_rocks.jpg
64      mars_rocks.jpg
```

FIGURE 2 – List Function



Download

File Download

mars_rocks.jpg

List / Search of Files

```
File Name
61 mars_rocks.jpg
62 mars_rocks.jpg
64 mars_rocks.jpg
```

FIGURE 3 – Search Function

My experience and education within the technology realm encompasses infrastructure/network/information security design, operations, and maintenance. I’ve avoided programming throughout my professional career. When dealing with developers in the workplace, I’ve always ensured I discuss work applicable to me and not dive into the development side of things. After this collaborative project, I find myself diversifying my professional portfolio, combining my existing skillsets with programming – DevSecOps. Our organization is working on developing an in-house Work Order management system, requiring us to integrate our IT and OT systems. This module has equipped me with the knowledge as well as the interest to dive deeper into the development side for our project instead of shying away from it. I still have more to learn, but like this project has taught me, I’ll learn from doing it with time.

The IT market requires professionals to have multiple skillsets from different domains under their belt. With digital transformation on many organizations’ strategic roadmap, building on my development skills will aid me in my current role as well as set me up for success in my career to follow.

References

Chieu, T., Mohindra, A., Karve, A. and Segal, A., 2009. Dynamic Scaling of Web Applications in a Virtualized Cloud Computing Environment. *2009 IEEE International Conference on e-Business Engineering*, [online] Available at: <https://ieeexplore.ieee.org/document/5342101> [Accessed 21 May 2022].

Markandey, A., Dhamdhere, P. and Gajmal, Y., 2018. Data Access Security in Cloud Computing: A Review. *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, [online] Available at: <https://ieeexplore.ieee.org/document/8675033> [Accessed 19 May 2022].

Mhaskar, N., Alabbad, M. and Khedri, R., 2021. A Formal Approach to Network Segmentation. *Computers &amp; Security*, [online] 103. Available at: <https://www.sciencedirect.com/science/article/pii/S0167404820304351> [Accessed 21 May 2022].

Tsochev, G., Trifonov, R., Manolov, S., Nakov, O. and Spasov, S., 2021. Analysis of Threats to a University Network Using Open Source Technologies. *2021 International Conference Automatics and Informatics (ICAI)*, [online] Available at: <https://ieeexplore.ieee.org/document/9639729> [Accessed 22 May 2022].