



Knight Foundation School of Computing and Information Sciences

Spring 2023 Senior Design Project

Capstone Project Selection Secured by AWS

Students: Fares Almoshaikah

Instructor/Faculty: : *Dr. Seyedmasoud Sadjadi*, Florida International University

PROBLEM

The current process for capstone project selection involves the professor distributing an unsecured Excel sheet link to students. Accessing an unsecured Excel sheet creates a security and integrity risk as anyone with access can alter the information contained within it. Additionally, unauthorized access to the Excel sheet can lead to a breach of sensitive student and faculty information. These problems can lead to incorrect data being presented and hinder the overall group forming and project selection process.

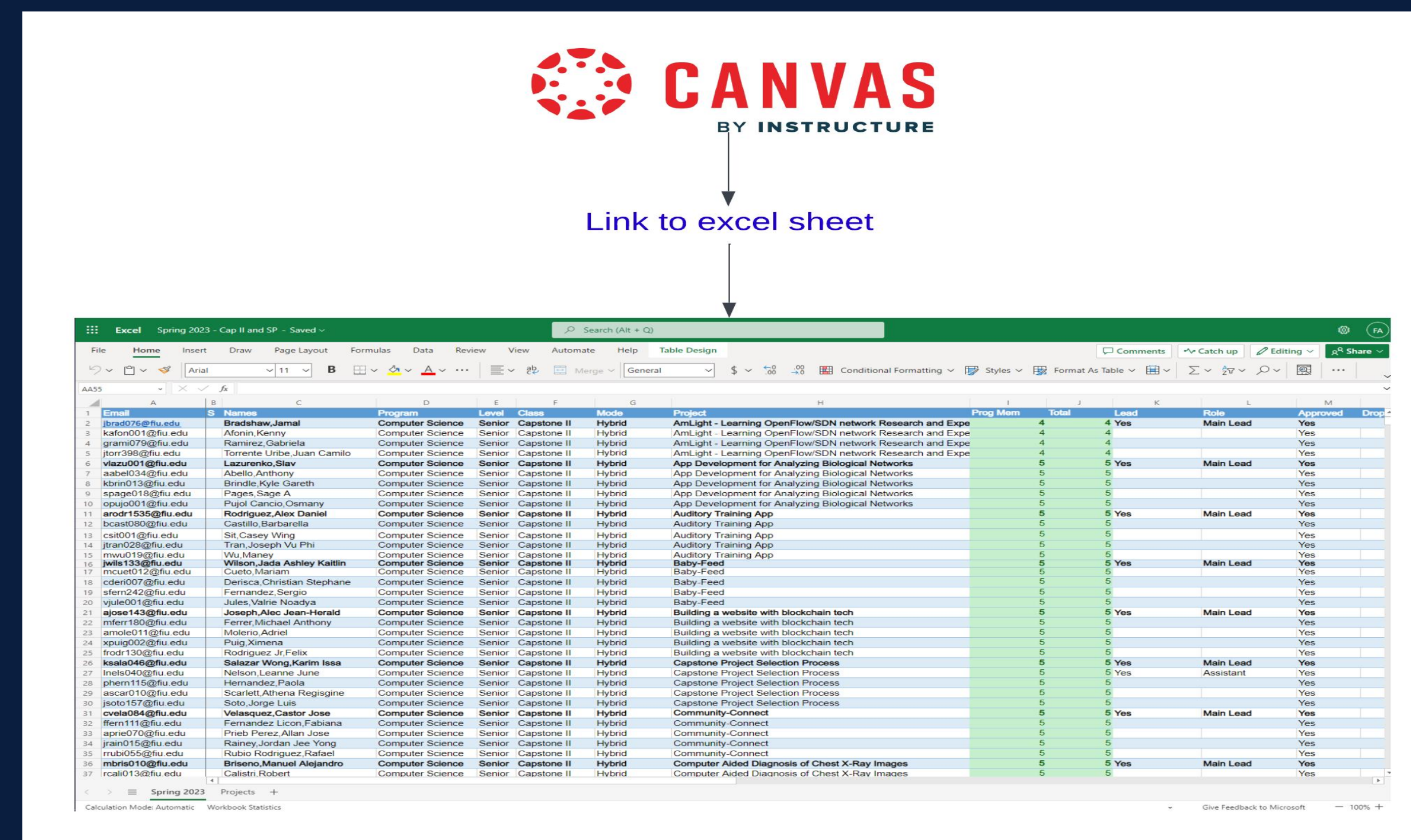
REQUIREMENTS

- Determine a more secure way of hosting the capstone project selection sheet
- Utilize what was learned from AWS Academy Cloud Security Foundations in our solution
- The system must provide secure access to the capstone project selection process
- User authentication must be required to access the system
- The system must be secure
- The system must be scalable
- The system must be highly-available
- All access to the system must be logged with the ability to be audited.

RECOMMENDATIONS

- Move selection process off excel hosted by Microsoft Sharepoint and use an SQL database hosted on an RDS
- Modify inbound and outbound rules to prevent ports from being accessible from internet gateways.
- Use FIU SSO
- Implement auto scaling groups so ec2 instances can be terminated or deployed as load increases or decreases
- Use Cognito User pool and incorporate Lambda triggers to ensure only FIU Capstone Cohort is given access

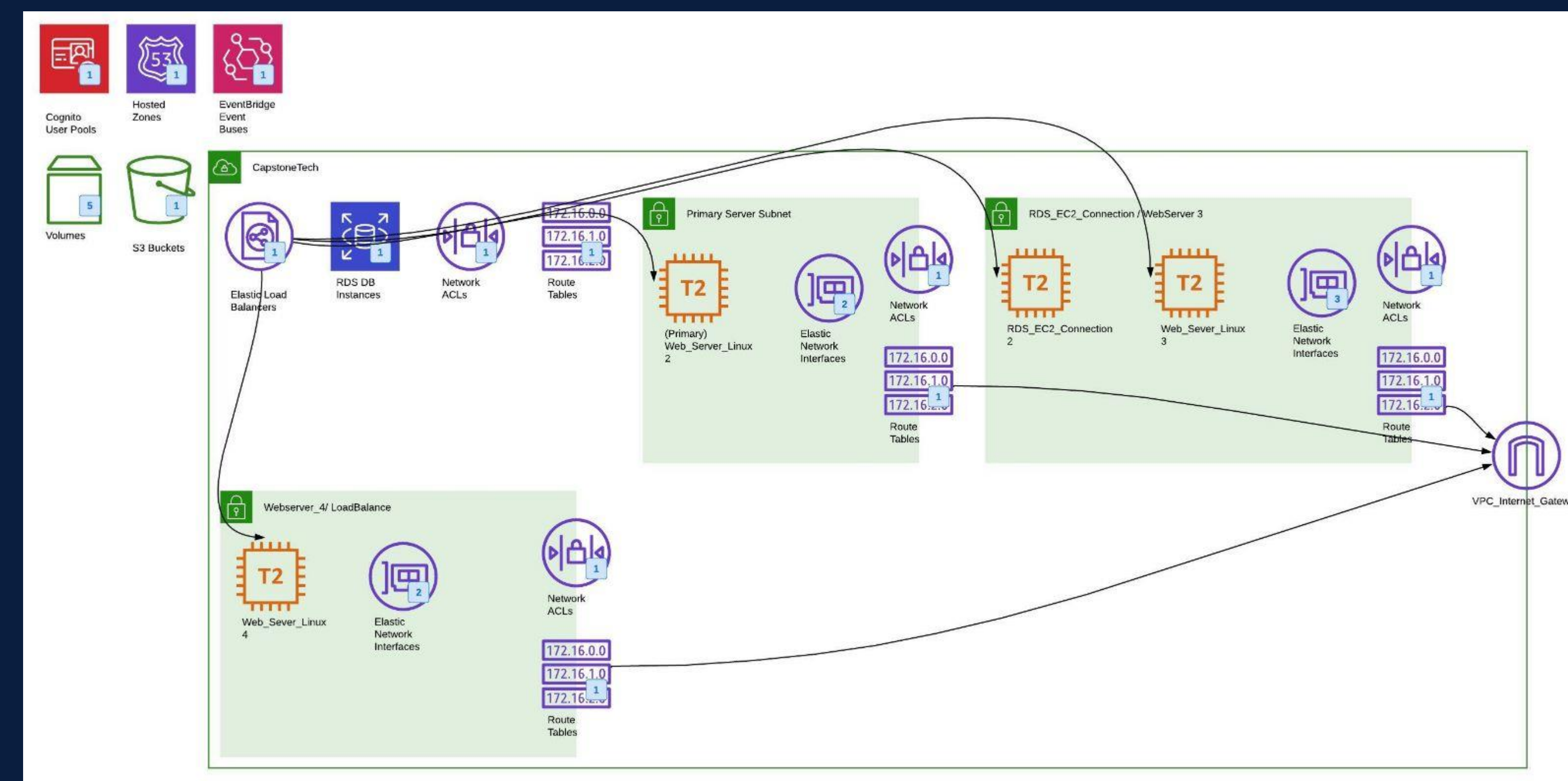
CURRENT SYSTEM



RISK ANALYSIS

	Negligible	Moderate	Severe
Very Likely	Student signs in using non-FIU account	Students alter other student's information	Student deletes all information on excel
Somewhat Likely	Student signs in using another student's account	Student accesses AWS account that hosts the website and resources	Student emails classmates fake link leading to malicious site
Unlikely	Non-FIU student signs in and alters information	Students to DDOS server	Students access AWS using unsecure ports (80, 443, 3306, 22)

SYSTEM DESIGN



SUMMARY

In this project, we utilized Amazon's EC2 service to create multiple VPCs to host our capstone project selection website. The website features a secure login page that requires students to authenticate using their FIU credentials before gaining access to the selection excel sheet. By leveraging the capabilities of EC2 and other AWS services such as Cognito, S3, RDS DB, Elastic Load Balancers, and EventBridge event buses, we were able to implement a comprehensive and effective set of controls to manage risks and threats in our cybersecurity project. This ensured the security, reliability, and resilience of our systems and data.

SECURITY CONTROL IMPLEMENTATION

- Implemented Multiple Virtual Private Clouds (VPCs) to host our capstone project website front-end
- Set up Cognito to manage user authentication and authorization
- Utilized two-factor authentication
- Migrated data from excel to an AWS RDB secured instance
- Implement CloudTrail to audit and monitor activity logs
- Implement CloudWatch for real-time monitoring of the health of the EC2 instances.
- Implement auto-load balancing to ensure availability of project selection process during high-load periods
- Stored and secured data for website front-end via an S3 bucket.

REFERENCES

- Amazon Web Services. (n.d.). AWS Documentation. Retrieved from https://docs.aws.amazon.com/?nc2=h_ql_doc_do
- Amazon Web Services. (n.d.). Amazon Elastic Compute Cloud (EC2). <https://aws.amazon.com/ec2/>
- Amazon Web Services. (n.d.). Amazon S3. <https://aws.amazon.com/s3/>
- Amazon Web Services. (n.d.). Amazon RDS. <https://aws.amazon.com/rds/>
- Amazon Web Services. (n.d.). Amazon Cognito. <https://aws.amazon.com/cognito/>