CSCI 5409 – Cloud Computing

Security & Business Considerations Critical Analysis and Response

Work done by,

GROUP 31

- **Guturu Rama Mohan Vishnu – B00871849**
- **Aditya Deepak Mahale – B00867619**
- **Sumit Singh – B00882103**

Question 1:

How does your application architecture keep data secure at all layers? If it does not, if there are vulnerabilities, please explain where your data is vulnerable and how you could address these vulnerabilities with further work.

Answer:

We are using VPC private subnet to protect out user data and making sure that no one other than the authorized person has the access to user's personal data. On top of it we are also using security group to secure our RDS database by only allowing mysql/auroraDB connection type from our EC2 instance only, we are ensuring this by using private subnet from VPC. In the code, we are using Django inbuilt hashing to secure the data which will travel over the network this helps us avoid traffic eavesdropping threat. Talking about audio file that's stored in the s3 bucket, it has public access for now. And it is prone to security vulnerability. But we are not storing the s3 file url and making it one time retrievable for authorized user. This way we are making sure no one can get their hands on the audio file except the user who produced it or the person he wants to give access to. Further to increase the security we can also make it one-time downloadable file once the user translates the input. This way we won't even have to expose our s3 bucket url.

Question 2:

Which security mechanisms are used to achieve the data security described in question 1? List them, and explain any choices you made for each mechanism (technology you used, algorithm, cloud provider service, etc.)

Answer:

We are using VPC, private subnet, security group, Django inbuilt hashing. For transport layer protection of data and data at rest, we are using Django inbuilt hashing operation. Hashing is one way non reversable form of data protection. It is important to protect data while it is transferred over the network and also data at rest.

We are ensuring least privilege by implementing different security groups for each service and also ensuring separation of authorization by doing so. We are allowing mysql/auroraDB connection for Database, this ensures least privilege and also separation of authorization.

We are also using VPC to secure out services in different layers. In our project only EC2 instance call connect to our RDS and no other service is allowed to communicate it.

Question 3:

What would your organization have to purchase to reproduce your architecture in a private cloud while providing relatively the same level of availability as your cloud implementation? Try to give a rough estimate of what it would cost, don't worry if you are far off. These systems are complicated and you don't know all the exact equipment and software you would need to purchase. Just explore and try your best to figure out the combination of software and hardware you would need to buy to reproduce your app on-premise.

Answer:

Our architecture design includes three main layers for communication with the client. In addition, we are utilizing AWS Polly and translation services in the backend. To reproduce a similar configuration on-premises, it would require the following components.

- ✓ 1 Bare metal server for the front-end deployment.
- ✓ 1 Load balancer for the API layer
- ✓ 2/3 bare metal servers for the API deployment.
- ✓ 2 Bare metal servers for the database deployment- Along with enterprise edition support of one of the databases (Oracle or PostgreSQL (EDB))
- ✓ On-premise network devices such as routers, switches, firewalls, wireless LAN, etc.
- ✓ 2 high-performing bare metal servers for hosting machine learning services for audio conversion and language translation. These servers would also require multiple graphic processing units.
- ✓ On-premise storage for hosting binary files.

The below pricing shows the investment for a year.

- **Bare metal server deployments:**

A bare metal server initial investment would cost around $ 40,000 for the first year.

Maintenace and labour charges would cost $ 9000/year.

The project requires 1 (Frontend) + 2 (API)

Cost: 3 x 40000 = **$ 120000**

- **Load balancer:**

A NGINX Plus load balancer would do the job of load balancing traffic at the API layer. A single load balancer would serve the purpose.

The project requires 1 NGINX Plus load balancer

Cost: 1 x 15500 = **$ 15500**

- **Oracle Database Server + License:**

The standard edition of the oracle database server would be needed for the Django application in the API layer.

The project requires 1 database server.

Cost: 1 x 29750 = **$ 29750**

- **On-premise network setup:**

The entire network needs to be set up from scratch for the project.

The network setup would approximately cost **$ 20000**

- **Machine learning GPUs + Server:**

Audio conversion and text translation requires high performance computing platform. Hence, it requires servers with multiple cores and GPUs.

Two servers would be required in the project.

Cost: 2 x 26000 = **$ 52000**

- **Hosting binary files:**

Min.io provide an alternative storage for S3.

Cost: **$ 12000**

Question 4:

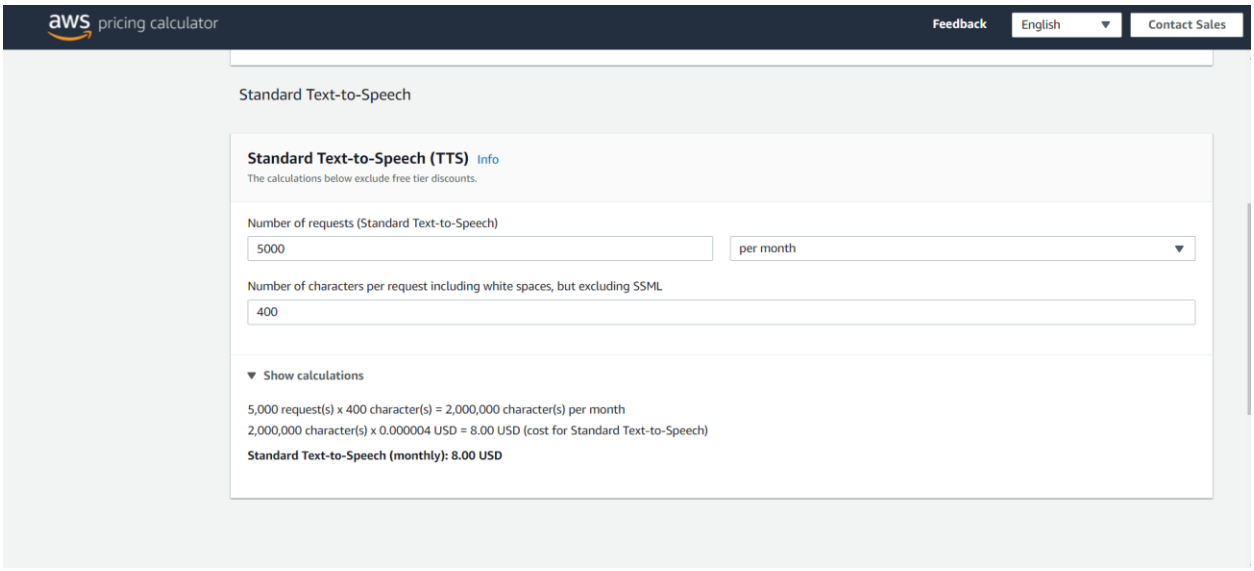
Which cloud mechanism would be most important for you to add monitoring to in order to make sure costs do not escalate out of budget unexpectedly? In other words, which of your cloud mechanisms has the most potential to cost the most money?

Answer:

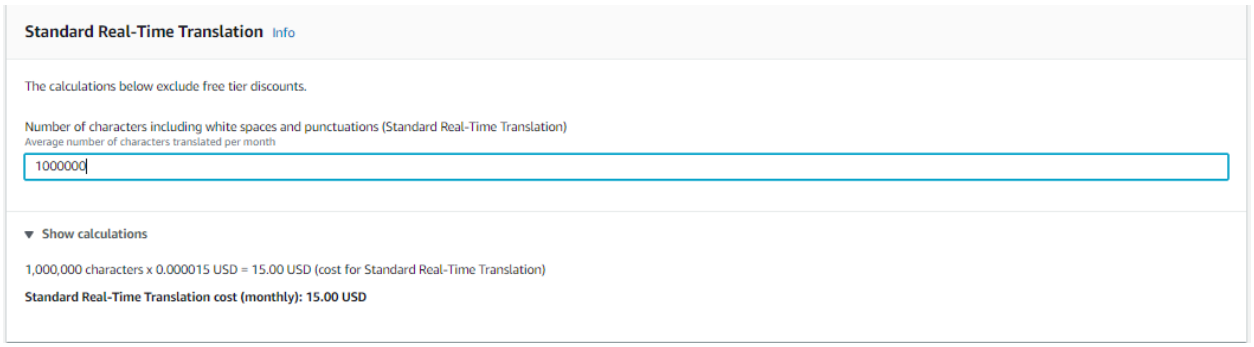
In our project, the important mechanism to be monitored would be Polly, Translate and S3. The reason for this is that, our entire application is based on Polly and Translate. Every time a user sends in a text and hits the result button, our application will trigger Polly and Translate and also S3, in order to store the translated audio files in the bucket. So, the more number of times the user tries, the more times these services are going to be called. But in order to constrain our costs within the budget, we are planning to implement an auto-erasing feature in our S3 bucket. It means, every audio file which a user has translated their text into, will be first stored in S3 and then it will be auto-deleted from the bucket after 30 days. This way, we can try to minimize our costs and control the budget within our calculations.

Below are the images depicting the amount monthly to manage all the three major services of our application.

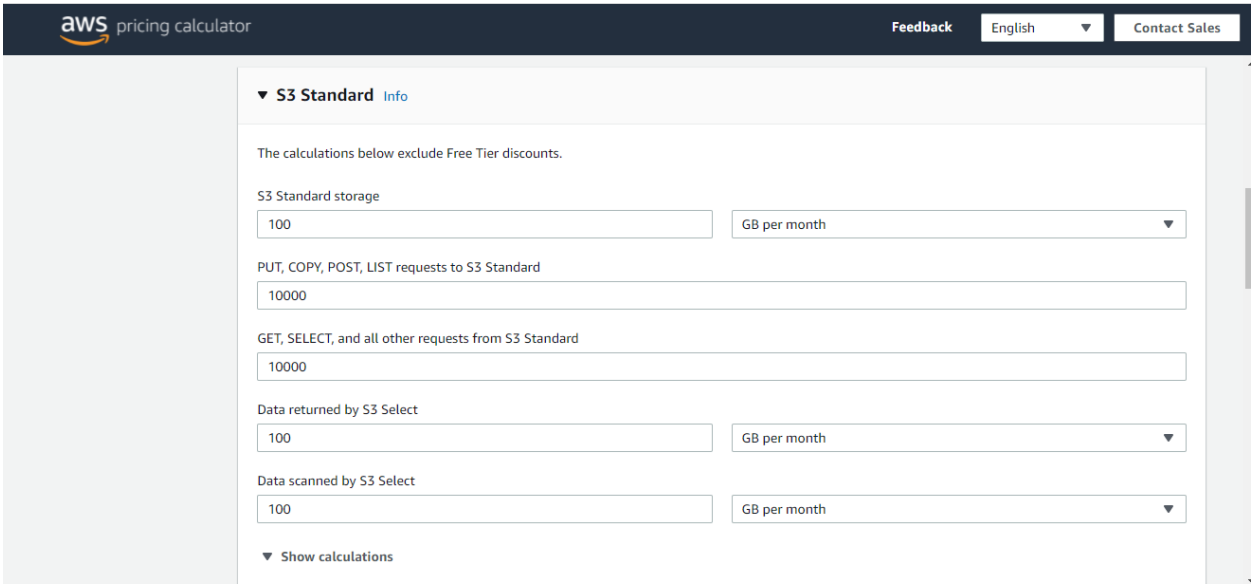
For Polly,



For Translate,



For S3,



▼ **Show calculations**

Tiered price for: 100 GB

100 GB x 0.0230000000 USD = 2.30 USD

Total tier cost = 2.3000 USD (S3 Standard storage cost)

10,000 PUT requests for S3 Storage x 0.000005 USD per request = 0.05 USD (S3 Standard PUT requests cost)

10,000 GET requests in a month x 0.0000004 USD per request = 0.004 USD (S3 Standard GET requests cost)

100 GB x 0.0007 USD = 0.07 USD (S3 select returned cost)

100 GB x 0.002 USD = 0.20 USD (S3 select scanned cost)

2.30 USD + 0.004 USD + 0.05 USD + 0.07 USD + 0.20 USD = 2.62 USD (Total S3 Standard Storage, data requests, S3 select cost)

S3 Standard cost (monthly): 2.62 USD

References:

[1] "*Total cost of ownership of servers,"* Sherweb [Online]. Available at: https://www.sherweb.com/blog/cloud-server/total-cost-of-ownership-of-servers-iaas-vs-on-premise/ [Accessed: March 26, 2022].

[2] "*Oracle DB Licensing Calculator*," Wintelguy.com [Online]. Available at: https://wintelguy.com/oracle-db-licensing-calc.pl [Accessed: March 24, 2022].

[3] "*AWS Pricing Calculator,"* Calculator.aws [Online]. Available at: https://calculator.aws/#/createCalculator/Translate [Accessed: March 29, 2022].

[4] "*Amazon Polly*," Amazon Web Services [Online]. Available at: https://aws.amazon.com/polly/ [Accessed: March 29, 2022].

[5] "*Cloud Object Storage – Amazon S3 – Amazon Web Services*," Amazon Web Services [Online]. Available at: https://aws.amazon.com/s3/ [Accessed: March 29, 2022].