# MIDTERM

**Student Name:** Shoumit Rajnish Karnik

**University ID:** 116717496

**Course ID:** ENPM809J

**Course Name:** Cloud Security

## EXECUTIVE SUMMARY

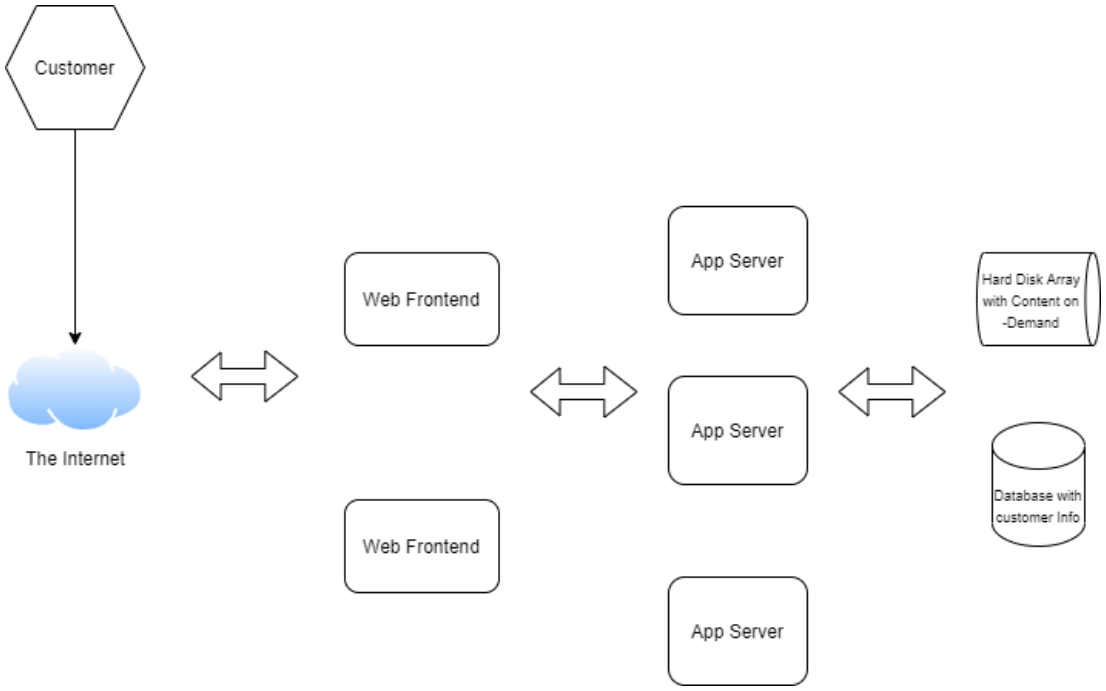
In this document the strategy, which will be adopted to redesign the Cobra Kai web streaming service to take advantage of the benefits of moving to the cloud, has been outlined. The purpose for re-engineering the application from an on-premises hosting platform to a cloud-based infrastructure and database platform was to increase security, reduce outages and downtime and compliance with PCI-DSS standards.

## ISSUES AND CONSIDERATIONS

The customer is an on-premises streaming platform which streams live and on-demand training sessions to clients worldwide. With the increased acceptance of the platform, the customer felt that the current architecture was limited with respect to scaling their on-premises data center. More specifically, their closet server is now inept of scaling up or out. There are numerous security issues in their current system as well which will be outlined subsequently.

- Patching strategy missing
- Backup strategy missing
- Account permission strategy missing (Identity and access management (IAM) required)
- Availability of services at risk of compromise (System resilience (Integrated enterprise risk management) to be implemented)
- Load balancing strategy missing
- PCI DSS compliance issues

## CURRENT SYSTEM ARCHITECTURE

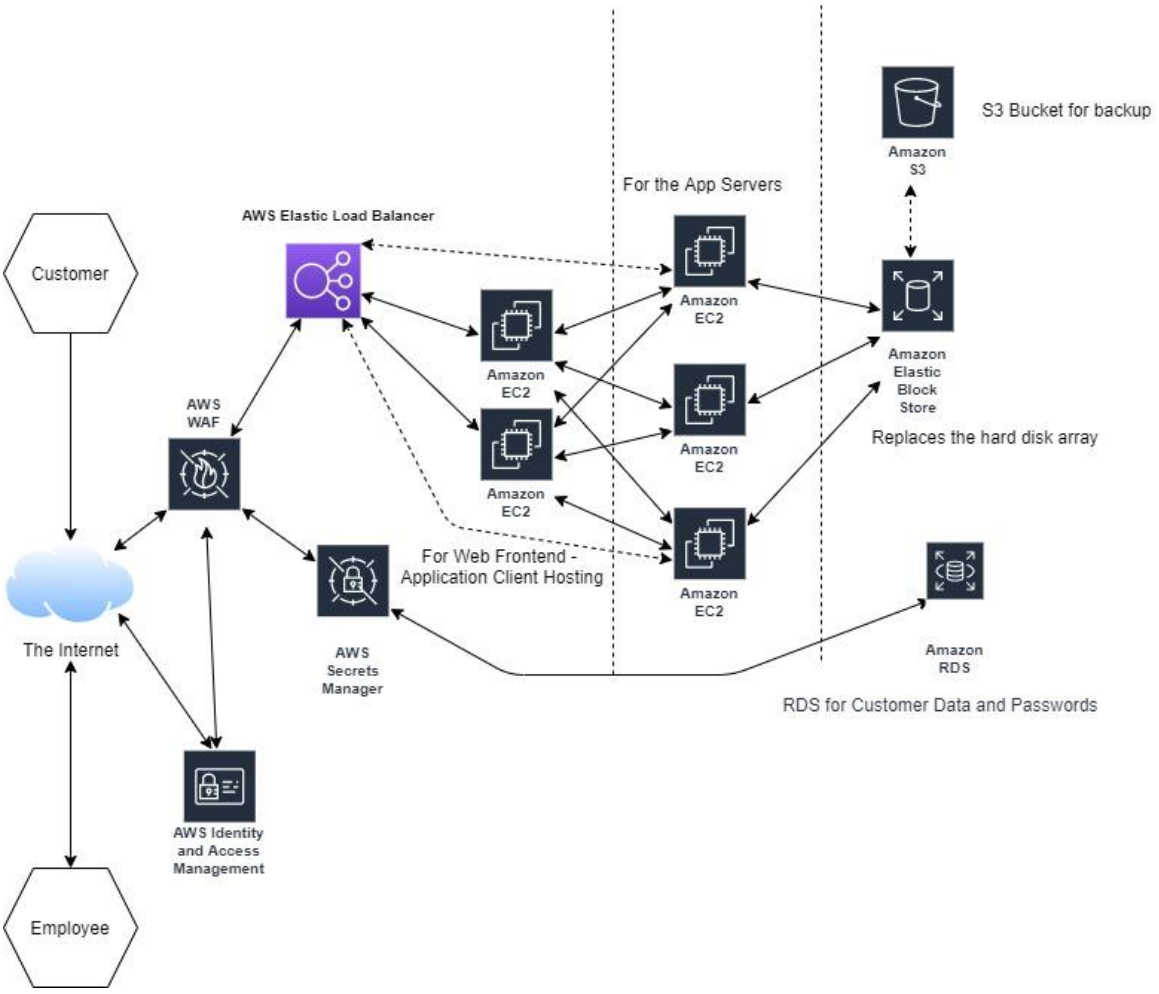



## PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture is a single-cloud solution with a combination of re-architecting and re-platforming strategies. The cloud vendor used for the solution is AWS(Amazon Web Services).

1. Necessary but minimal changes to the core code are proposed. Only the data layer needs to be changed and a new module for scaling and load balancing is introduced. Also, a web application firewall is really recommended because cloud security on its own is not enough.
2. The Cloud services in-built Identity and Access Management module will be used to provide better access control and role assignment to take care of unauthorized accesses to the website.
3. Patching and backup will be handled by the AWS's own respective patch and backup managing services.
4. Multi-dimensional application front-end layer (support for multi-tenant hosting) is proposed.
5. Multi-feature servers (Hosting instances of the application servers) are proposed.
6. Distribution across region-based infrastructure for geographical context-sensitive load balancing is proposed which will result in better throughput and streaming quality for subscribers. It will also lead to better resiliency and disaster recovery against DDoS attacks.

The subsequent sections of the document explain the key architectural changes and how they would be deployed on the cloud infrastructure.




## PROPOSED SOLUTION DETAILS

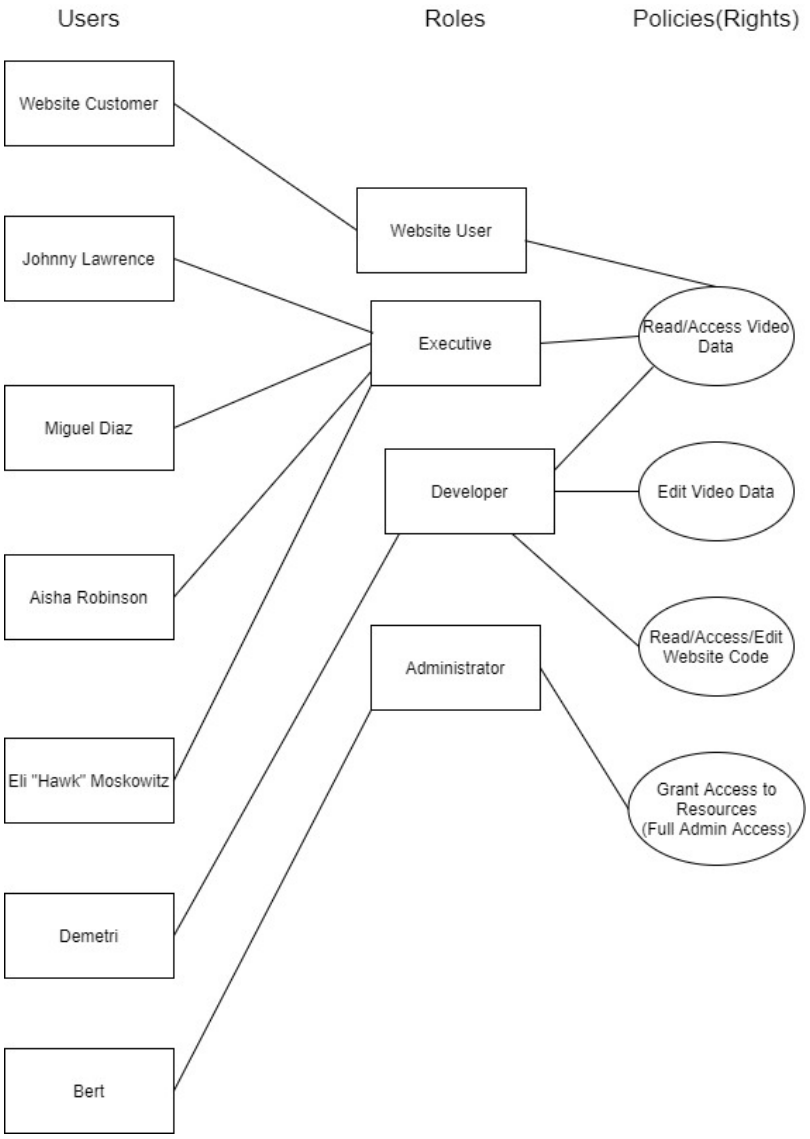
### AWS WAF(Web Application Firewall)

This is a firewall which will be deployed before or on the Load Balancer, which will serve as the first line of defense from attackers for the system. This approach will help filter out any unnecessary requests and using signatures will help prevent common web attacks like cross site scripting and website request forgery.

### AWS IAM(Identity and Access Management)

AWS Identity and Access Management is used to make a list of users for the website and its resources and to decide the level of access granted to each role.

A simple RBAC diagram will explain how the roles will be assigned to various company employees and users of the website.




This is just the initial layout of the how the accesses should be configured using the AWS IAM Console. However as and when required later, the System Administrator(Bert), having administrator root privileges, can assign new people roles, or grant people temporary access to files they require using policies.

## AWS Secrets Manager

The secrets manager will be used to encrypt and securely store customer data using rolling keys. This will ensure that customer card information is safe as well as their other data like names, phone numbers are not leaked in case of an attack. This will also help make the system PCI-DSS compliant.

## AWS Elastic Load Balancer

The company has been suffering outage problems and has been suffering from DDoS attacks. To counter these problems and to also ensure proper scale-out of systems along with maximum worldwide

availability and throughput, the AWS Elastic Load Balancer is being used. This will ensure scalability, availability, and protection against a Distributed Denial of Service(DDoS) attack.

### Amazon EC2 (Along with Amazon EC2 Systems Manager for patching)

The current Web Frontend instances and the Application servers are being handled on-premises. These are proposed to be moved to cloud EC2(Elastic Compute Version 2) instances to ensure compatibility with the other cloud services that we need to apply.

The other benefit of using EC2 is the EC2 Systems Manager which will help the System Administrator develop proper patching schedules and apply them whenever they are due. This will make the entire system more secure.

### Storage - Amazon Elastic Block Store(EBS), Amazon Relational Database Service(RDS) and Amazon Simple Storage Service(S3)

The storage, as opposed to the current hard disks, will be handled by cloud completely.

Amazon EBS is proposed for the storage of the company product data i.e. the streaming videos. This storage was chosen because of two key reasons:

- This type of storage provides fast streaming access along with providing easy scaling solutions even if the sizes of the videos were to increase.
- Along with EBS snapshot service, it provides a simple backup solution.

Since the backup is stored in the form of block files, a simple S3 bucket is used for storing the backup.

The Amazon RDS is used in place of the on-premises database to store customer secrets inclusive of names, credit card numbers and contact numbers. This is used in conjunction with the AWS Secrets manager to protect customer data and achieve PCI compliance.

## SOLUTION WORKFLOW

A typical website workflow is as follows:

- The customer will first create an account on the website. When this happens, they will be assigned the Website user role and their credentials and payment information will be stored in the RDS database.
- Whenever the customer logs back in their supplied username and password will be compared with the value in the RDS for validation and if successful they will be given access to the EBS videos.
- The way the customer loads will be handled will be configured on the Elastic Load Balancer. A load balancer accepts incoming traffic from clients and routes requests to its registered targets (such as EC2 instances) in one or more Availability Zones.
- The load balancer also monitors the health of its registered targets and ensures that it routes traffic only to healthy targets.

- When the load balancer detects an unhealthy target, it stops routing traffic to that target. It then resumes routing traffic to that target when it detects that the target is healthy again.
- The health parameter is based on the amount of load the EC2 instance is handling at that point in time.
- The multi-tenant framework of the Application frontend and the Web Servers also makes sure that the load balancer is used effectively and the process of accessing a video from the database is smooth and efficient.
- The AWS IAM will ensure that customers (or users) are able to access only files which they have been given the permission to access. It also ensures that employees also handle only those files which pertain to their work.

## PROS AND KEY BENEFITS

- Dynamically scalable solution with small operational overheads which operates across geographies.
- Leverages Amazon's infrastructure and builds around available solutions thereby reducing investment and maintenance.
- All costs are pay as you go, thereby reducing a big upfront solution cost.
- Proper patching and backup strategies in place thereby preventing any disruptions to availability or security
- Proper Identity and Access Management in place thereby reducing the risk by internal or external threats.
- System is more resilient due to various security features in place as well as by implementing the load balancer.
- Customer secrets are now properly encrypted and stored.
- With a lot of the security risks mitigated, system is more PCI-DSS compliant.

## CONS AND RISKS

- Single vendor used, hence there is a risk of vendor tie-in.
- Administration tasks still handled by company employee; misconfiguration can lead to introduction of new vulnerabilities.

## FUTURE SCOPE

- The company (Cobra Kai) is advised that in the future they should move towards a multi-cloud strategy, to avoid vendor tie-ins and provide an even better disaster management plan and a better, more resilient framework. Due to budget constraints, a single cloud strategy with minimal security is proposed, for protection of customer data in accordance with the 12 key concepts of PCI.

- For further DDoS resiliency, services like Amazon CloudFront, Route53 and API Gateway can be used to ensure better availability.
- The Secrets Manager can be used to manage access to secrets using fine-grained AWS Identity and Access Management (IAM) policies and resource-based policies.
- Furthermore, to enhance streaming capabilities, services like Amazon CloudFront and Amazon Elastic Transcoder can be used to enhance the streaming experience for customers.

**NOTE:** AWS was chosen because of the services being cheaper and more cost-effective when compared with other cloud platforms like Microsoft Azure and GCP.

## REFERENCES


https://aws.amazon.com/waf/

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

https://aws.amazon.com/iam/

https://aws.amazon.com/rds/

https://aws.amazon.com/s3/

https://aws.amazon.com/ec2/?ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

https://aws.amazon.com/ebs/?ebs-whats-new.sort-by=item.additionalFields.postDateTime&ebs-whats-new.sort-order=desc

https://aws.amazon.com/systems-manager/

https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1603478065257

https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html