



A. JAMES CLARK  
SCHOOL OF ENGINEERING



# COBRA KAI REARCHITECTURE

## High-Level Technical Design

---

**Version 2.0**

**12/18/2020**

*Strike First - Strike Hard - No Mercy*

**Author:** Kevin Mukam

**Email:** kevinmukam@gmail.com

Cloud Security

# Table of Contents

<b>1. Introduction .....</b>	<b>5</b>
<b>2. Current System .....</b>	<b>6</b>
2.1 Functional Description.....	6
2.2 User Community Description .....	7
2.3 Technical Architecture.....	8
<b>3. Goals, Objectives, and Basis for Modified System .....</b>	<b>9</b>
3.1 Project Purpose.....	9
3.2 Goals and Objectives .....	9
3.3 Proposed System .....	9
3.3.1 Summary of Changes.....	12
<b>4. Factors Influencing Technical Design .....</b>	<b>14</b>
4.1 Assumptions .....	14
4.2 Constraints .....	14
4.3 Design Goals .....	14
<b>5. Proposed System .....</b>	<b>16</b>
5.1 High-Level Operational Requirements and Characteristics .....	16
5.1.1 User Community Description .....	16
5.1.2 Secure Cloud Practices .....	17
5.1.3 Availability Requirements.....	17
5.1.4 Volume and Performance Expectations .....	18
5.2 Cloud Provider .....	18
5.2.1 Video Storage and Streaming.....	19
5.2.2 Data Protection.....	20
5.2.3 Security Groups & Firewalls.....	21
5.2.4 IAM Groups/Roles for Cobra Kai.....	22
5.2.5 Coding Practices .....	23
5.2.6 Resiliency .....	24
5.2.7 Patching .....	24
<b>6. Analysis of the Proposed System .....</b>	<b>26</b>
6.1 Impact Analysis .....	26
6.1.1 Operational Impacts .....	26
6.1.2 Organizational Impacts .....	26
6.2 Risks.....	27

6.3	Critical Success Factors for Remainder of Project .....	27
<b>Appendix A: Conceptual Information Model .....</b>		<b>29</b>
<b>Appendix B: Record of Changes .....</b>		<b>30</b>
<b>Appendix C: Acronyms.....</b>		<b>31</b>
<b>Appendix D: Glossary .....</b>		<b>32</b>
<b>Appendix E: Referenced Documents .....</b>		<b>33</b>
<b>Appendix F: Approvals .....</b>		<b>34</b>
<b>Appendix G: Revision History .....</b>		<b>35</b>

## List of Figures

Figure 1 – Cobra Kai’s Website (Home) .....	6
Figure 2 – Cobra Kai Leadership.....	7
Figure 3 – Cobra Kai’s Current Website Architecture .....	8
Figure 4 - Proposed Architecture for Cobra Kai.....	12
Figure 5 – Responsibility in the Cloud .....	17
Figure 6: AWS .....	19
Figure 7 - Real Time File Processing .....	19
Figure 8 - Real-Time Stream Processing.....	20
Figure 9 - AWS Key Management Service .....	20
Figure 10 - Security Group Approach in AWS.....	21
Figure 11 - Security Group for Cobra Kai Instances .....	22
Figure 12 - Cobra Kai AWS IAM Groups .....	22
Figure 13 - Policies for IAM Users in the Admins Group .....	23
Figure 14 – AWS Resilience .....	24

Figure 15 - High-Level Conceptual Information Model .....	29
---	----

## **List of Tables**

Table 1 - User Community Description .....	16
Table 2 - Record of Changes .....	30
Table 3 - Acronyms .....	31
Table 4 - Glossary .....	32
Table 5 - Referenced Documents .....	33
Table 6 - Approvals .....	34
Table 7 - Revision History .....	35

# 1. Introduction

---

With the evolution of the internet, the increase in the internet population and the need for data protection, companies are redirecting their services from their premises to Cloud Storage. According to a study from Tech Jury, 85% of businesses worldwide are already making use of cloud technology to store information. With services such as data protection, cost efficiency, regulatory compliance, scalability, accessibility, resiliency and other benefits that will be discussed in this document, cloud operations have become one of the most important features for the future of companies.

For the daily operations and growth of Cobra Kai Karate Dojo, moving to the cloud will be fundamental. In order to migrate to the cloud, redesigning Cobra Kai's current website architecture is essential. By rearchitecting the application, Cobra Kai's cloud applications will support future growth more effectively than applications that aren't modified. Also, redesigning the application to be cloud native will be a learning experience for the information technology (IT) team. This will positively change the IT team's culture, as they adapt to working with dynamic, flexible, on-demand cloud features.

An example of a popular application that was rearchitected before cloud migration is Netflix. Netflix spent an extended period of time on their cloud migration on application rearchitecting, rather than rushing to the cloud. Netflix benefited from the effort, which totally reshaped their internal technology and even their operations model. Today, they find themselves well positioned to support the company's business growth and future expansion.

This document lays emphasis on the technical plan for moving Cobra Kai application to the cloud, specifically to Amazon Web Services (AWS). Factors like resiliency, identity and access management (IAM), data protection, compliance, large files handling, secure system administration and coding practices are discussed.

## 2. Current System

Cobra Kai is a successful karate dojo in Los Angeles, CA. The dojo has grown to be one of the most successful dojos in the United States. With increase in demand for karate training and COVID-19 restrictions, an online platform has been created to stream live and provide on-demand training sessions to members around the world.

The online karate class training program consists of a few servers in their data center. Demand has overtaken the processing power on the data center and there are security concerns about rivals who try to illegally gain access to the platform and data within the platform. With all that, the company has decided to migrate to the cloud.

Cobra Kai's current website architecture is a basic website architecture with hard disks that store on demand content, a database with customer information, application servers and a web frontend.



STRIKE FIRST - STRIKE HARD - NO MERCY



This the official site of Cobra Kai, a karate dojo in Reseda, Los Angeles, California! Please check out our [video](#) collections and purchase as many videos as you think make sense!

Figure 1 – Cobra Kai's Website (Home)

### 2.1 Functional Description

When Cobra Kai's customers connect to the website, they are connected to one of the front-end servers via round robin DNS (to load balance requests between the servers). After that, data is sent to one of 3 app servers for processing and the app server will either record data in a master database or send content stored on a hard disk array back to the user.

## 2.2 User Community Description

The users of the current system are broken down into customers, general employees and administrators.

The customers are the ones who externally access the website, watch streaming videos of the online karate classes offered by Cobra Kai and provide their PII (Personally Identifiable Information) and credit card information to buy videos. They can access the website from anywhere in the world.

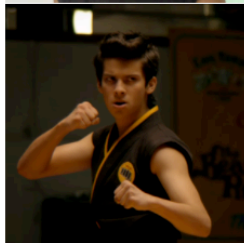
The general employees monitor the day-to-day operations of Cobra Kai. Their influence on the website is limited, they also provide PII and credit card information.

The administrators monitor the operations of customers, employees and the network. They consist of the founder of Cobra Kai, the Chief Operating Officer, the Chief Information Security Officer, the Chief Information Officer and the System Administrator.



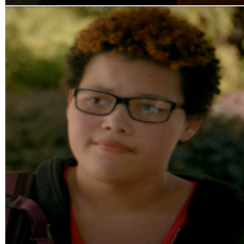
**Johnny Lawrence- CEO**

The founder of Cobra Kai and the visionary disrupting karate and karate training with the introduction of his streaming platform for karate training



**Miguel Diaz – Chief Operating Officer**

Miguel is the person in charge of daily operations for Cobra Kai and its streaming platform.



**Aisha Robinson - CISO and Head of Corporate Security**

Aisha is the enforcer for Cobra Kai both in person and online. Her security and risk focused mindset helps her discover and mitigate risks before they are exploited.



**Eli "Hawk" Moskowitz - Chief Information Officer**

"Hawk" is the brains behind the development of Cobra Kai's streaming platform

Figure 2 – Cobra Kai Leadership

## 2.3 Technical Architecture

The current architecture of the system consists mainly of a web frontend, app servers, a database and hard disks.

The front end of the website is the part that the customers interact with. Everything that they see when navigating around Cobra Kai's website, from fonts and colors to dropdown menus and sliders, the karate videos and all the services, are a combo of HTML, CSS, and JavaScript being controlled by their web browsers.

The app server collaborates with the web server to return a dynamic, customized response to a browser's request. It sits between the network and the database. It is designed to install, operate and host applications and associated services for the customers and IT services. The app server also provides Cobra Kai a certain layer of security. By sitting between web pages and databases, it acts as an additional barrier to SQL injection cyber-attacks as there is no direct link between the web page and the database.

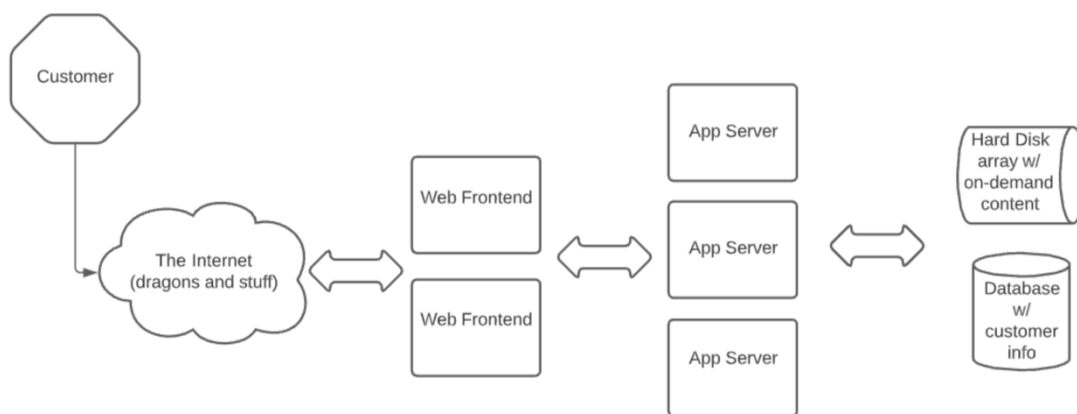


Figure 3 – Cobra Kai's Current Website Architecture

However, the system requires more security given the lack of firewalls, Identity & Access Management (IAM), and other security measures which will be discussed in further sections.

The database stores the customer's PII and credit card information. Surprisingly, the site does not have any PCI-DSS compliance for credit card processing, or privacy measures for customer PII.

The hard disk stores karate videos and on-demand content that is used by customers all around the world to download and pursue their online training sessions.



### **3. Goals, Objectives, and Basis for Modified System**

---

With the continuous growth of Cobra Kai, it is important to challenge the current issues that the organization is facing. The idea is to apply traditional security elements like firewalls and intrusion detection, to prevent direct rivals and unknown attackers to access Cobra Kai's data. The goal is to redesign the current website architecture to provide a better and more secure system before migrating to the cloud.

#### **3.1 Project Purpose**

Redesign the Cobra Kai application to take advantage of the benefits of moving to the cloud, especially with regards to security. Propose solutions for resiliency, identity and access management (IAM), data protection, compliance, large file handling, secure system administration and coding practices.

#### **3.2 Goals and Objectives**

By redesigning the architecture, the objectives are:

- Providing data protection.
- Handling large files for storage and streaming.
- Identity and Access Management.
- Complying to regulation laws.
- Reducing the attack surface.
- Enabling scalability.
- Practicing secure system administration.
- Enabling resiliency.

#### **3.3 Proposed System**

The proposed system consists of various important components. There are two firewalls, an external firewall and an internal firewall. This is to protect the company's network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data.

Single Sign-On (SSO) is added for customers and employees. With SSO, the users are able to log in just one time every 24 hours with one set of credentials to gain access to Cobra Kai's apps and website. SSO provides greater security and user experience.

At certain points in the system, honeypots are installed. A honeypot is a tool used to detect, isolate and analyze attacks by attracting attackers. It is a dummy machine with useless data, partially secured and configured as if it was a realistic portion of the production environment. When attackers penetrate it and attempt malicious activity, the security team can monitor and record the attackers' behavior. This information can be used for defensive purposes.

After being authenticated and authorized to access the resources, the users access the web application frontend. Authentication process verifies that users are who they say they are (password and a second authentication method) and authorization verifies that users have access to what they are trying to access with the help of an Access Control List (ACL). The web frontend executes code inside the web browser. HTML, CSS and JavaScript make up the frontend system.

Additional servers are setup. This is to reduce the attack surface. Requests for the backend arrive at the app server and are passed on the backend code. The backend is the part of the web app that is not visible to the customers. The backend receives requests, prepares the data (karate videos) and transmits to the browser.

The PII and credit card information are obtained and stored in compliance with U.S. laws for the cloud. Credit card storage follows PCI-DSS (Payment Card Industry Data Security Standards). PCI-DSS ensures that all companies that work with credit card data in any way (accepting, processing, storing, etc.) can maintain a certain level of cyber security within the environment.

Compliance to GDPR (General Data Protection Regulation) laws is added for Cobra Kai customers based in Europe. GDPR is a European Union law regulation that focuses on data protection and privacy on the territory of the EU (European Union) and EEA (European Economic Area).

Another law to follow is the DMCA (Digital Millennium Copyright Act). The DMCA is an anti-piracy statute making it illegal to bypass copy protections designed to prevent pirates from duplicating digital copyrighted works and selling or freely distributing them. With this addition, Cobra Kai's rivals such as Daniel LaRusso will be in trouble if they attempt to illegally access the platform and copy their techniques.

An Identity and Access Management (IAM) platform is created and an IAM administrator will be in charge of these operations. It is important for Cobra Kai to have IAM because there has to be control of authentication, authorization, user management and central user repository. The IAM administrator manages and optimizes secure IAM solutions, policies, roles, and technical controls to align Cobra Kai's business processes with compliance requirements. Cobra Kai will function in the cloud with a system of least privilege, users will be given minimum access and

permissions to perform their duties. Roles and policies will be assigned to various IAM Groups (see section 5).

Patching and Load balancing are implemented. Patching fixes vulnerabilities on applications that are susceptible to cyber-attacks. It also ensures that the applications are kept up to date and run faster. Patching is also a way of adhering to certain compliance standards.

Load balancing enables distribution of traffic across the additional servers. This ensures that no server bear too much demand. By spreading the network load, this improves the application's responsiveness, reduces downtime and increases performance.

Log Management is included. This is important to monitor employees' actions, to identify and solve problems, to show suspicious activity and also for regulatory compliance. PCI-DSS and other regulatory requirements require tracking of access to some systems that contain regulated data. Log management serves as a way to meet key regulatory compliance mandates.

The karate videos which consist of large files will be handled in the cloud. A service in AWS called Lambda will be important in handling these large files. AWS S3 and AWS Kinesis will also be used for video storage and streaming.

Data will be protected by encryption techniques. Encryption will be done for data at rest and data in transit. EBS in AWS will be important in data protection. For data in transit, everything will be TLS encrypted. Additional cloud services such as Security Groups, AWS Key Management System or Macie will be used. Secure coding practices will be enforced.

The proposed architecture for Cobra Kai is shown on figure 4 below.

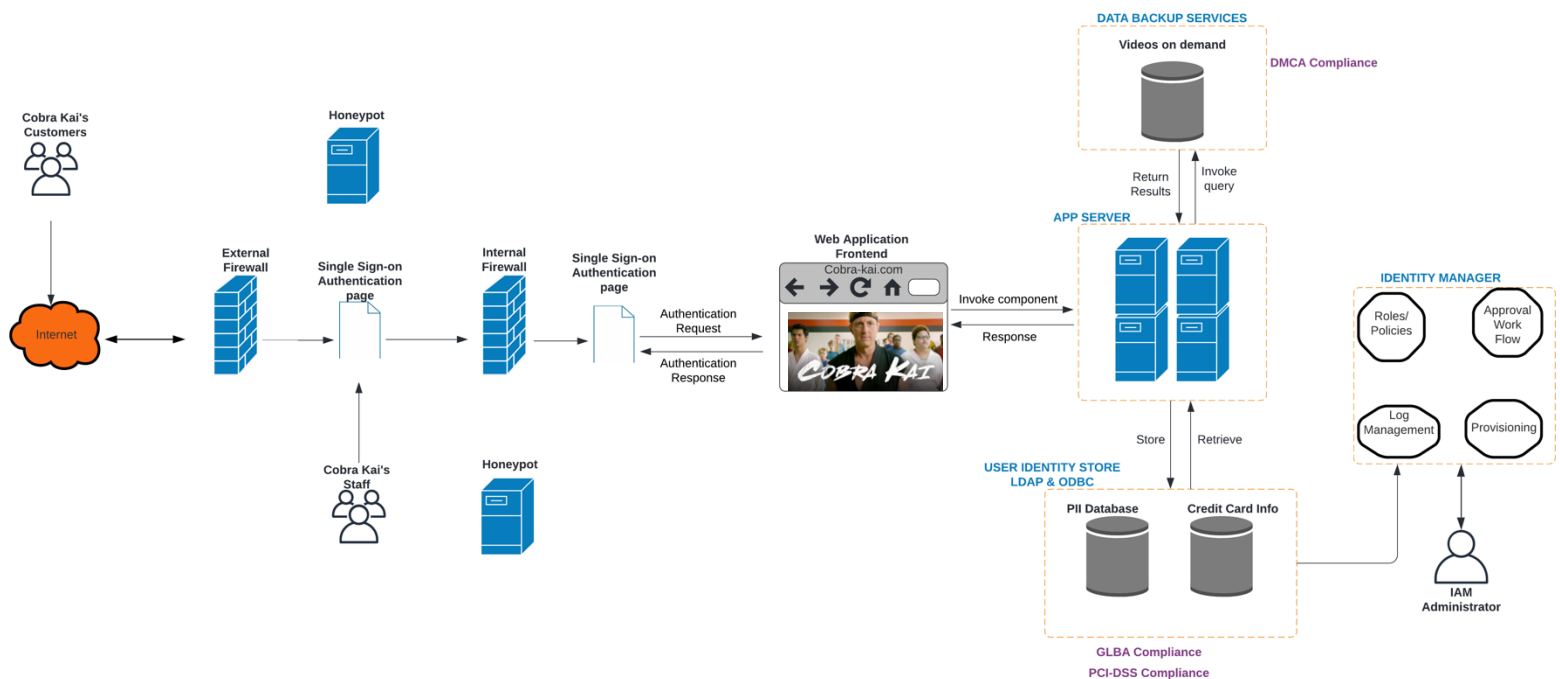


Figure 4 - Proposed Architecture for Cobra Kai

Cobra Kai will use sandboxes. A protected area where to test untested code or untrusted data. This could be of good use when reviewing resumes from applicants, because by receiving several pdf files from trusted and untrusted people, a malicious person can try to gain access to the systems by hiding malware inside a pdf.

### 3.3.1 Summary of Changes

- Firewalls are added to protect the network and filter unwanted traffic.
- Servers are added to provide load balancing and to reduce the attack surface.
- Identity and Access Management (IAM) is implemented to authenticate, authorize, manage users and serve as a central user repository.
- Log management is added to monitor employees' actions, show suspicious activity and for regulatory compliance.
- Compliance rules are observed for every sensitive data.
- Regular patching is implemented.
- Security Groups are configured for Cobra Kai.

- IAM policies and roles are implemented and regularly updated.
- Use of several AWS tools like CloudTrail, CloudWatch, Lambda, S3, EBS, to increase security and file handling.

## 4. Factors Influencing Technical Design

---

This section describes the assumptions and constraints that influence the technical design of the proposed system.

### 4.1 Assumptions

It is assumed that Cobra Kai doesn't have SIEM (Security Information and Event Management). SIEM provides real-time analysis of security alerts generated by applications and network hardware.

While the primary role of IAM is to provide identity assurance, SIEM collects authorization events and ingests logs from endpoints, firewalls, applications, and servers to determine what actors are actually doing within an enterprise.

### 4.2 Constraints

The following constraints influenced the decisions during the application redesign:

- No load balancing system for the available servers.
- Too many downtimes due to the increase in application popularity and few resources (not enough servers).
- No log management.
- No backup strategy.
- No account permission strategy, every user has the ability to run privileged commands (huge risk).
- No patching process for Operating Systems and software.
- No compliance to any laws.
- Large video files.

### 4.3 Design Goals

The new system must provide a high level of security. Not only against potential attackers, but also within the organization's staff. There must be a clear hierarchy on who has access to what, and limited access to sensitive operations.

Identity and Access Management to provision, manage and deprovision identities. Manage the user life cycle (customers and staff).

Log management. The addition of an IAM Administrator will be of huge benefit to Cobra Kai. Log management will be important to perform security checks, correlate events and meet compliance requirements.

Security Groups which are literally virtual firewalls. This is for the instances to control inbound and outbound traffic.

Resize and compress large video files. The event-driven computing platform called AWS Lambda will process data immediately after an upload. AWS Lambda and Amazon Kinesis will also be used to process real-time streaming data for application activity tracking, order processing, click stream analysis, metrics generation, social media analysis and IoT device data telemetry and metering.

Resiliency. Cloud resilience is understood as a way to readapt to a crisis situation. This applies to infrastructure and data. Cobra Kai's new environment will have an ability to recover from a potential failure induced by load, attacks and failures.

## 5. Proposed System

As stated in the aforementioned sections, the system will consist of firewalls that will filter incoming traffic, honeypots to serve as tools to detect and isolate attackers, authentication requests and responses managed by an Identity and Access Management Administrator, application servers that will receive requests from the frontend web pages and provide the required information stored in the backend.

Refer to Section 3.3 for additional detail.

### 5.1 High-Level Operational Requirements and Characteristics

#### 5.1.1 User Community Description

Table 1 below gives a brief explanation of users who make up the system.

Table 1 - User Community Description

User Group	Description	Type	Total Users
Users/ Customers	Watch karate videos online; provide PII and credit card info.	User	
General Employees	Day-to-day operations of Cobra Kai.	Employee	20
Development Team	Technical staff responsible for the information technology division of the company.	Employee	8
IAM Administrator	Authenticate, authorize and manage users in the system.	Admin	2
Leadership Team	Drive the business decisions.	Admin	2

These users are split into groups, where each group has their policies. Separating them in groups will allow Cobra Kai's IT department to manage users in bulk based on their job function, organizational unit and access needs. A user can be in more than one group.

New users will have no privilege at first. Cobra Kai will function with a system of least privilege, so that new users will have minimum levels of access and permissions to the system. Access to sensitive data will be logged.



### 5.1.2 Secure Cloud Practices

Cobra Kai's IT staff and all employees will be responsible for security in the cloud. However secure the system is designed, there is no 0 risk situation. The users will always be potential risk elements, either voluntarily or involuntarily, so regular cyber security trainings will be important. The system will store PII and credit card information, therefore there will have to be compliance to PCI-DSS laws, GDPR laws, DCMA laws for copyright and also a Privacy Policy section on the website to disclose Cobra Kai's practices on protecting personal information, but also to show users that the organization can be trusted, and that there are procedures in place to handle their personal information with care.

Cloud vendors as shown below function with a shared responsibility model. The cloud vendor is responsible for security of the cloud, but Cobra Kai will ultimately be responsible for security in the cloud.

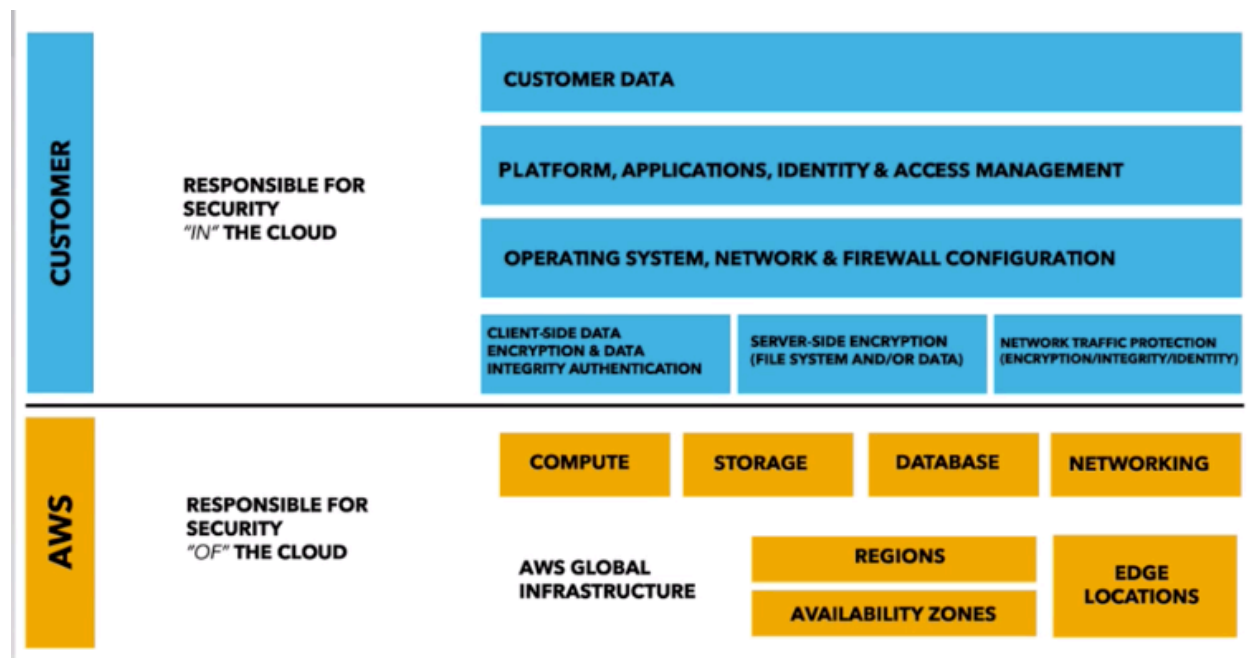


Figure 5 – Responsibility in the Cloud

### 5.1.3 Availability Requirements

Working on the cloud will solve the problem of trying to resolve an outage. In case there is an outage in the cloud, Cobra Kai will have back up servers that will run at most as soon as the outage occurs.

The downtime in the cloud shows up to 99.91% availability per year or simply put 7.75 hours of unavailability. With the on-premises backup servers and database at Cobra Kai, a potential unavailability of cloud services will be taken care of on the premises.

### 5.1.4 Volume and Performance Expectations

During the summer, Cobra Kai should expect the highest volume of customers. With the summer vacation, the favorable weather, the tourists and other factors, there will be a peak during the summer. Cobra Kai's computing needs won't remain static; there will be new (and hopefully more) users, customers, and data as the organization grows.

The addition of servers in the premises will play an important part during such times. An increase in the number of customers will be monitored effectively. Performance will not decrease, and security will still be ensured.

The cloud will also meet those needs in a much more cost-efficient manner than a traditional environment, because new computing resources will be assigned and allocated without any significant additional capital investment on the part of the cloud provider.

## 5.2 Cloud Provider

The cloud platform to host Cobra Kai's architecture is Amazon Web Services (AWS). In addition to the security that the rearchitected model provides, AWS provides security and file handling.

AWS also offers flexibility and affordability. A preferred operating system can be chosen, web application platform, programming language. This eases migration from the current platform. Also, all services offered by the company are affordable and billed on a per-use basis. There are no upfront payments or contracts.

Services such as CloudTrail in AWS are important for log monitoring. CloudTrail records every API call made and stores it (every 5 minutes). Also, a service such as CloudWatch is used for monitoring AWS resources, operations and security. Access Control Lists (ACL) will also be created for Cobra Kai inside the AWS environment.

There are a lot of benefits in working with this cloud provider, whose architecture can be summarized in figure 6.

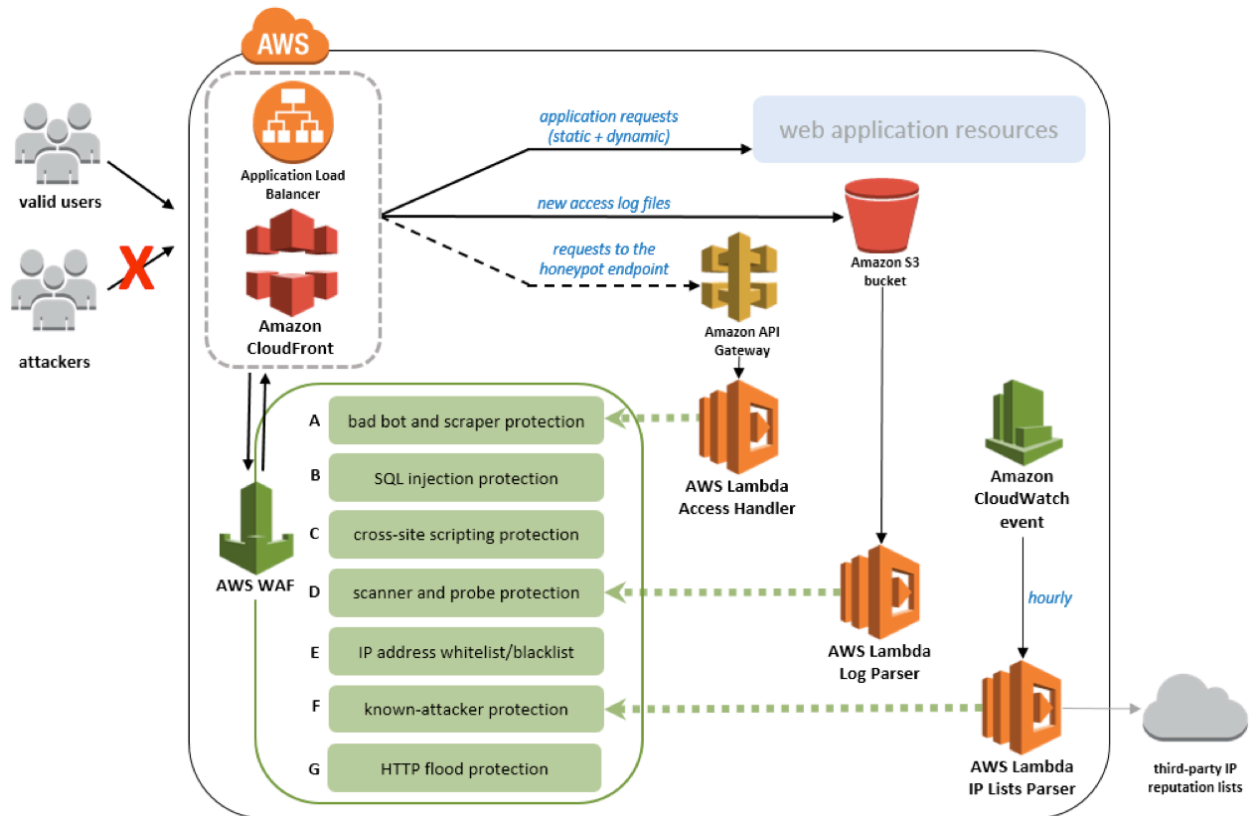


Figure 6 – AWS

### 5.2.1 Video Storage and Streaming

The videos will be stored in Amazon S3 (Simple Storage Service). S3 is for object file storage that can be easily accessed. It is scalable, highly available and has low latency. It will give the IT team access to highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites.

Given the nature of the large video files, AWS Lambda will be used. It is an event-driven computing platform. It runs when triggered by an event and executes code that's been loaded into the system. Every time a karate video will be uploaded into S3, a Lambda function will automatically compress and resize the video.



Figure 7 - Real Time File Processing

The event that triggers the Lambda function is the file being uploaded to S3. Lambda then executes the function of compressing and resizing the image.

Lambda and Amazon Kinesis will also be used to process real-time streaming data for application activity tracking, transaction order processing, click stream analysis, data cleansing metrics generation, social media analysis, indexing and log filtering.



Figure 8 - Real-Time Stream Processing

The social media stream is loaded into Kinesis in real-time and Lambda runs code that generates hashtag trend data and stores it in Dynamo database.

For long term storage of data that will be infrequently accessed, Amazon Glacier can be used. It is cheaper than S3 and data can be accessed in minutes. Also, in terms of security, it supports IAM permissions and data is encrypted.

## 5.2.2 Data Protection

Data created outside AWS will be encrypted before transferring to the cloud or during transit. Data created in AWS will be encrypted all the time. AWS has a Key Management Service (KMS) which handles creation, management, and deletion of keys used to encrypt data. AWS only uses symmetric encryption (one key to open them all). Amazon EBS (Elastic Block Store) enables encryptions at rest. EBS provides snapshots (copy of data at a point in time). The snapshot is stored in S3.

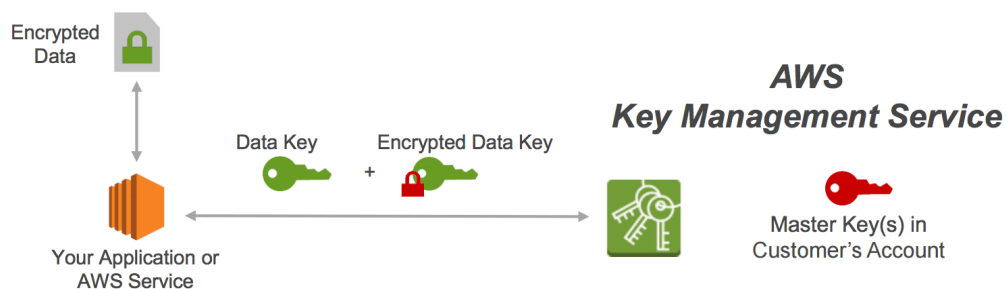


Figure 9 - AWS Key Management Service

Amazon has a service called Macie which uses machine learning to identify, classify and protect sensitive data in AWS. It can identify PII and intellectual property. It is a powerful security and

compliance service that provides an automatic method to detect, identify, and classify data within AWS.

### 5.2.3 Security Groups & Firewalls

Security groups are the central component of AWS firewalls. They act as virtual firewalls, controlling incoming and outgoing traffic in AWS. Security groups will be attached to the network interface of EC2 instances on startup. By default, they deny inbound traffic. Rules created are only to allow traffic in.

The security groups will follow a naming convention with the notation '**AWS Region + Environment Code + OS Type + Tier + Application Code**'. Proper naming convention is a simple practice but makes the AWS experience better. For example:

- Security Group Name: CA-D-LWA001
- AWS Region (2 chars): EU, VA, CA etc.
- Environment Code (1 char): P – Production, T – testing, D – Development, etc.
- OS Type (1 char): L – Linux, W – Windows etc.
- Tier (1 char): W – Web, A – App, C – Cache, D – Database etc.
- Application Code (4 chars): A001

Amazon has services such as CloudTrail and CloudWatch Flow logs. The IT department will use CloudTrail to record every AWS API call (which will record it to an S3 bucket). CloudTrail tells you who made the call, when it was made, what was the call, what were the resources used and where it was made. It checks for creation, deletion, modification of security groups, changes to IAM policies, S3 bucket policies, failed logins, and launching/termination of EC2 instances.

Cobra Kai will make use of CloudWatch Flow Logs to record each time a packet enters or leaves a virtual private cloud (VPC). It enables cloud customers to capture information about the IP traffic going to and from network interfaces in their VPC. Flow log data does not affect network throughput or latency.

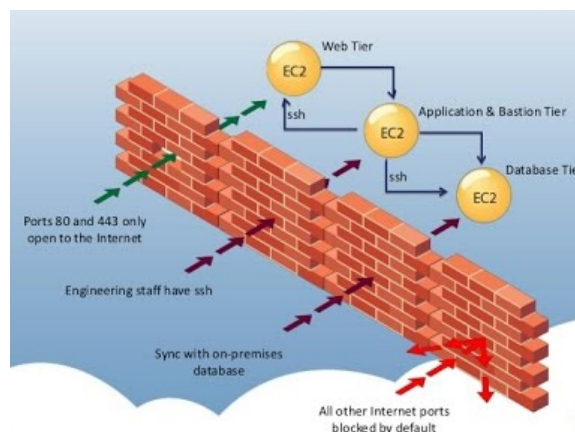


Figure 10 - Security Group Approach in AWS

Below is a sample security group that will be used for Cobra Kai instances in the subnet 172.16.112.0/24:

The screenshot displays the AWS Management Console interface. At the top, the 'Instances (1/1)' section shows a single instance with ID 'i-0b91d67a876d2d101' in a 'Running' state, using a 't2.micro' instance type. Below this, the 'Security groups' tab is selected, showing a list of rules for the security group 'CA-D-LWA001'. The rules are as follows:

Port range	Protocol	Source	Security groups
80	TCP	172.16.112.0/24	CA-D-LWA001
22	TCP	172.16.112.0/24	CA-D-LWA001
5000	TCP	172.16.112.0/24	CA-D-LWA001
443	TCP	172.16.112.0/24	CA-D-LWA001

Below the inbound rules, the 'Outbound rules' section shows a single rule:

Port range	Protocol	Destination	Security groups
All	All	0.0.0.0/0	CA-D-LWA001

Figure 11 - Security Group for Cobra Kai Instances


### 5.2.4 IAM Groups/Roles for Cobra Kai

A primary use for IAM users is to give people the ability to sign in to the AWS console for interactive tasks and to make programmatic requests to AWS services. An IAM group is a collection of IAM users. The groups will be used to specify permissions for a collection of users. At this moment in time, three distinct Cobra Kai groups have been created and given specific permissions.

<input type="checkbox"/>	Group Name ↕	Users	Inline Policy	Creation Time ↕
<input type="checkbox"/>	cobrakai-admins	0		2020-12-16 01:30 EST
<input type="checkbox"/>	cobrakai-dev	0		2020-12-16 01:31 EST
<input type="checkbox"/>	cobrakai-general	0		2020-12-16 01:31 EST

Figure 12 - Cobra Kai AWS IAM Groups

The users in the admin group will have policies like “Database administrator”, “System administrator”, “Administrator access and Network administrator”. The IAM administrator will manage the groups, roles and policies.


Group ARN: arn:aws:iam::064805056662:group/cobrakai-admins 

Users (in this group): 0

Path: /

Creation Time: 2020-12-16 01:30 EST

Users Permissions Access Advisor

Managed Policies 

The following managed policies are attached to this group. You can attach up to 10 managed policies.

[Attach Policy](#)





Policy Name	Actions
 DatabaseAdministrator	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>
 SystemAdministrator	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>
 AdministratorAccess	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>
 NetworkAdministrator	<a href="#">Show Policy</a>   <a href="#">Detach Policy</a>   <a href="#">Simulate Policy</a>

Figure 13 - Policies for IAM Users in the Admins Group

IAM Users in the developers' group will have policies such as AWS Code Build Developer Access or Developer Authenticated Identities. In the cobrakai-general group, IAM Users will only have read only access.

Additionally, with AWS CloudFormation, Cobra Kai's developers can allow resource lifecycles to be managed repeatably, predictably and safely while managing resources across accounts and regions. CloudFormation template will be used to create, update and delete an entire stack as a single unit as often as needed, instead of managing resources individually.

### 5.2.5 Coding Practices

Attention to secure coding practices can prevent vulnerabilities from being introduced when implementing and use an application. Cobra Kai's development team will have to keep good secure coding principles. This means, writing scalable and maintainable code, writing comments and providing a good documentation, reviewing the code every time there is a meaningful change.

It is also recommended to practice pair programming, which will be a way for developers from the Cobra Kai team to learn from each other and enable the work to be double checked.

In addition to that, backup on code is very important to ensure that the code stays safe.

### 5.2.6 Resiliency

Resiliency refers to the ability of an architecture to continue providing the same quality of service even if some of its resources become inaccessible. For example, if one of Cobra Kai's web servers falls over, the website continues to work properly. AWS has several choices that provides architecture resilience.

AWS offers customers the ability to achieve highly resilient network connections between Amazon Virtual Private Cloud and the on-premises infrastructure. Highly resilient network connections are key to a well architected system. AWS recommends connecting from multiple data centers for physical location redundancy.

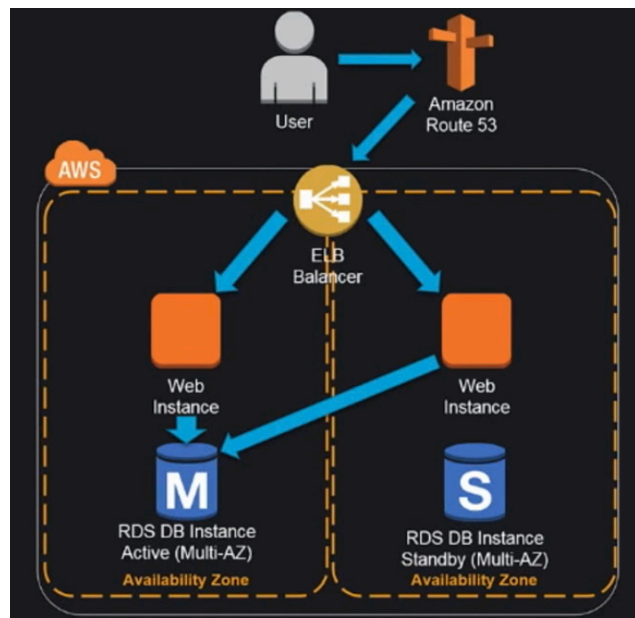


Figure 14 – AWS Resiliency

For more than 1000 users, Cobra Kai's web app will look like what is shown on figure 14. The more users there are on the web app, the more failover and redundancy arise. Having multiple availability zones resolves that problem. The latency between the availability zones is a few milliseconds.

Elastic Load Balancing (ELB) will enable the users to be divided between the two web instances depending on the traffic in each of the zones. In case one web server is unavailable, ELB will redirect the traffic to the other web server.

### 5.2.7 Patching

Patches are updates released generally to repair existing bugs or put preparations in place to prevent future ones. Cobra Kai's IT admins will have to implement a systematic way to control



how the systems are patched. AWS has a Patch Manager which automates the process of patching instances with both security related and other types of updates. Patch Manager can be used for both operating systems and applications. Patch Manager integrates with AWS IAM and CloudTrail to provide a secure patching experience that includes event notifications and the ability to audit usage.

Cobra Kai's IT admins will have the ability to control patches on remote user systems and remotely manage patches while out of the office. They will have to regularly scan for vulnerabilities and patches, and keep an up-to-date inventory of devices and servers.

Patch management is important for key reasons. It will increase security by fixing vulnerabilities on the operating systems and applications that are susceptible to cyber-attacks, it will increase system uptime by ensuring that applications are kept up-to-date, it aligns with compliance rules and also it improves software features. With a good patch management, Cobra Kai's online services will be a great tool for clients' satisfaction.

## 6. Analysis of the Proposed System

---

This section analyzes the proposed system and cloud migration by determining its impact on the organization, analyzing risks, and describing remaining issues.

### 6.1 Impact Analysis

#### 6.1.1 Operational Impacts

Implementing a load balancing system with more servers will increase availability of videos for customers.

Real-time stream processing with Amazon Lambda and Kinesis will provide timely insights to new information. This will allow Cobra Kai to process and analyze data as it arrives and respond instantly instead of having to wait until all data is collected before processing begins.

Low risk data that needs to be highly available will have to go to the cloud.

Keeping up with checklists daily.

The IT development team will review code regularly and keep good secure coding principles, logging everything and patching the Operating Systems.

All employees will have to report any suspicious emails to the IT department.

Solid workflow policies will include separation of duties and least privilege.

#### 6.1.2 Organizational Impacts

The current hierarchy will have to follow the new company guidelines in terms of permission strategy. The idea that every user could run privileged commands on the web server will not be possible anymore. Every general staff member and IT staff member will be subject to logging, Cybersecurity training and documentation.

Cobra Kai will have to implement Non-Disclosure Agreements (NDA) for all staff, to protect sensitive and confidential information from being shared or sold to anyone who is not supposed to legally receive that information. This will create a degree of trust and confidence within the organization, and also between the organization and its customers.

Prior to hiring, background checks should be performed, to protect Cobra Kai from a number of potential risks. For current employees, personnel policies should be used that include comprehensive training, job rotation and two-person integrity in situations where it makes financial and operational sense. Active surveillance and monitoring programs will be used.

Data should be masked and obfuscated for all personnel who don't need to work directly with raw data.

## 6.2 Risks

It is important to keep in mind that the human asset is the biggest risk. Simple errors such as a click on a phishing email could cause damage to the entire company. There are countless stories of employees who think that they have permission to perform a task, and they find themselves unintentionally exposing their company to exploitation.

**Multitenant Environment:** Working with a cloud provider means that Cobra Kai will be in the same environment with other organizations. The risks in this situation include conflict of interest (The cloud provider could possibly be in business with a competitor such as Daniel LaRusso). In a multitenant environment, other risks include escalation of privilege (authorized users may try to get unauthorized permissions) or information bleed (data belonging to one customer can be read by another).

Many potential risks are reduced by maintaining a certain level of control (hardware, software, personnel, security controls). However, this entails a great deal of expense and effort does not remove all risks. Moreover, since Cobra Kai is not primarily an IT company, it will mean more expense to hire IT specialists and administrators.

**Vendor Lock-In:** In ceding control of the production to the cloud, Cobra Kai creates dependency on the cloud provider, and dependency is a risk.

**Vendor Lock-Out:** It can be caused when a cloud provider goes out of business, is acquired by another business or ceases operation. To avoid a vendor lock-out when selecting a provider, the following will be considered: cloud provider longevity, core competency, legislative environment and jurisdictional suitability.

## 6.3 Critical Success Factors for Remainder of Project

The human factor is the biggest risk. It doesn't matter how secure the system is made, if someone decides to share their password, the system will be vulnerable. No matter the number of servers added or network administrators hired, keeping good security practices is vital. One way to mitigate this risk is training. Use incentive programs to identify personnel who resist social engineering attempts and bring them to the attention of the security office.

Sending data to the cloud is not the end of the road. Cobra Kai is still responsible for the safety of the organization's data. The ultimate legal liability remains with Cobra Kai. Unauthorized disclosure of PII or credit card information can cause huge problems in justice. Cobra Kai will have to hire knowledgeable, trained personnel with applicable skillsets. Another solution is deferring to general counsel in planning and managing the system.

Continuous monitoring of logs. Continuous patching. Continuous vulnerability scanning. Automation.

Entities outside Cobra Kai (like Daniel LaRusso) may want to attack the network for reasons such as competitiveness, political goals, perceived grievances, etc. These attacks can take many forms including DDoS, data breach, legal repercussions, and more. Therefore, Cobra Kai will be using protected devices and virtual machines with a strong security baseline and thorough configurations, as well as strong access controls. As the company continues to grow, Cobra Kai can solicit the services of a Threat Intelligence Service for better protection.

## Appendix A: Conceptual Information Model

Interrelated entities in Cobra Kai's business are shown below. Figure 3 shows the relationships between the entities in the Cobra Kai redesigned application. These entities have attributes that define their properties.

The entities are objects about which information is stored. Their relationships are represented by diamond shapes and they show how two entities interact. The attributes are represented by circular shapes and they are characteristics of entities.

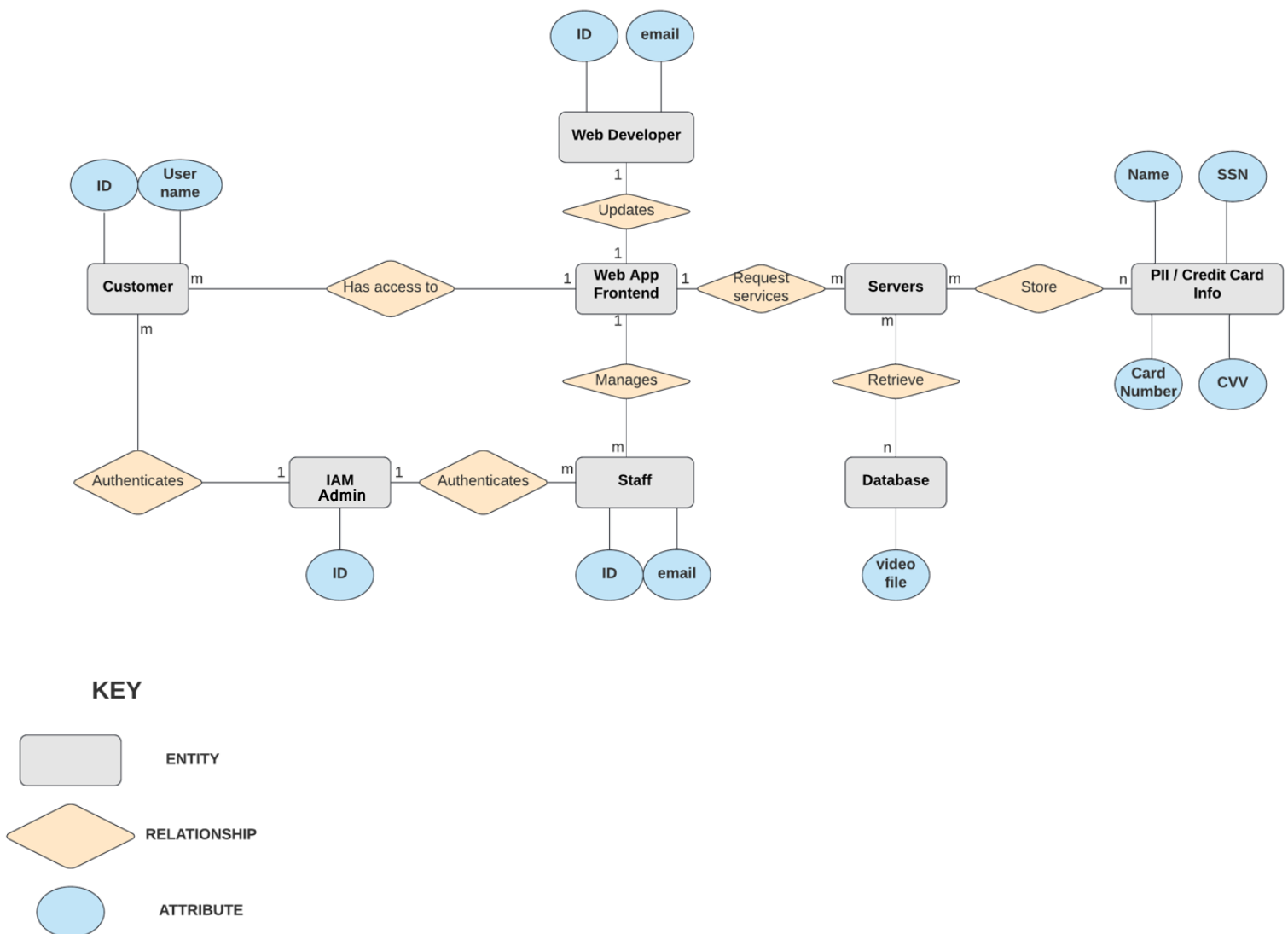


Figure 15 - High-Level Conceptual Information Model

## Appendix B: Record of Changes

Table 2 - Record of Changes

Version Number	Date	Author/Owner	Description of Change
1.0	10/23/2020	Kevin Mukam	Redesign of Cobra Kai's current (September 2020) architecture to a more secure and regulatory architecture.
2.0	12/18/2020	Kevin Mukam	Technical Plan / Road Map for moving the application to the cloud.

## Appendix C: Acronyms

Table 3 - Acronyms

Acronym	Literal Translation
ACL	Access Control Lists
API	Application Programming Interface
AWS	Amazon Web Services
CSS	Cascading Style Sheets
DMCA	Digital Millennium Copyright Act
DNS	Domain Name Server
EBS	Elastic Block Store
EC2	Elastic Compute Cloud
GDPR	General Data Protection Regulation
HTML	Hypertext Markup Language
IAM	Identity and Access Management
IT	Information Technology
KMS	Key Management Service
NACL	Network Access Control List
OS	Operating System
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
S3	Simple Storage Service
SIEM	Security Information and Event Management
SSO	Single Sign On
VPC	Virtual Private Cloud

## Appendix D: Glossary

Table 4 - Glossary

Term	Definition
<b>Authentication</b>	Establishes identity by asking who you are and determining whether you are a legitimate user.
<b>Authorization</b>	Evaluates what you have access to after authentication occurs (in many cases, this means comparing the identity assertion against an access control list).
<b>Attacker</b>	Individual or organization who breaches the information system of another individual or organization to perform some malicious activity and disrupt the network.
<b>Cloud</b>	Servers that are accessed over the Internet, and the software and databases that run on those servers.
<b>Cloud Provider</b>	A service provider that offers customer storage or software solutions available via a public network, usually the Internet.
<b>Cloud Customer</b>	The organization purchasing, leasing, or renting cloud services.
<b>Compliance</b>	Conforming to a rule, such as a specification, policy, standard or law.
<b>Database</b>	An organized collection of data, generally stored and accessed electronically from a computer system.
<b>Downtime</b>	Periods when a system is unavailable.
<b>Firewall</b>	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
<b>Honeypot</b>	A tool used to detect, identify, isolate, and analyze attacks by attracting attackers.
<b>Load Balancing</b>	Distributing network traffic across multiple servers to ensure that no single server bears too much demand.
<b>On-prem</b>	Software and a hardware infrastructural setup deployed and running from within the confines of an organization.
<b>Malware</b>	Any software intentionally designed to cause damage to a computer, server, client, or computer network.
<b>Patching</b>	Keeping IT systems and applications in the cloud or on-prem environment safe from malicious users that exploit vulnerabilities.
<b>Resiliency</b>	Ability to handle failures gracefully and recover the whole system
<b>Scalability</b>	The ability to increase or decrease IT resources as needed to meet changing demand.
<b>Security Groups</b>	Virtual firewall for an instance to control inbound and outbound traffic.
<b>Server</b>	A computer or computer program which manages access to a centralized resource or service in a network.
<b>Threat</b>	A potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
<b>Throughput</b>	An actual measure of how much data is successfully transferred from source to destination
<b>Vulnerabilities</b>	A weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries within a computer system.



## Appendix E: Referenced Documents


Table 5 - Referenced Documents

Document Name	Document Location and/or URL	Issuance Date
Cloud Adoption Statistics for 2020	<a href="https://techjury.net/blog/how-many-companies-use-cloud-computing/#gref">https://techjury.net/blog/how-many-companies-use-cloud-computing/#gref</a>	10/08/2020
Certified Cloud Security Professional: Official Study Guide	ISBN: 978-1-119-27741-5	04/27/2017
Cloud Outages: Cloud Services Downtime and The Lasting Impact	<a href="https://www.crn.com/news/cloud/index/cloud-outages-cloud-services-downtime.htm">https://www.crn.com/news/cloud/index/cloud-outages-cloud-services-downtime.htm</a>	2011
The 5 Benefits of AWS (And 3 Drawbacks) for Your Business	<a href="https://sados.com/blog/aws-benefits-and-drawbacks/">https://sados.com/blog/aws-benefits-and-drawbacks/</a>	2019
The Impact of Cloud Computing on Organizations in Regard to Cost and Security	<a href="https://www.diva-portal.org/smash/get/diva2:728880/FULLTEXT02">https://www.diva-portal.org/smash/get/diva2:728880/FULLTEXT02</a>	2012
The Organizational Impact of the Cloud	<a href="https://www.wired.com/insights/2012/11/the-organizational-impact-of-the-cloud/">https://www.wired.com/insights/2012/11/the-organizational-impact-of-the-cloud/</a>	2018
Human Error Is the Biggest Cyber Security Threat	<a href="https://bit.ly/2H6QeeZ">https://bit.ly/2H6QeeZ</a>	11/01/2019
WHAT ARE THE BENEFITS OF MONITORING EVENT LOGS?	<a href="https://www.graylog.org/post/what-are-the-benefits-of-monitoring-event-logs">https://www.graylog.org/post/what-are-the-benefits-of-monitoring-event-logs</a>	01/31/2019
Moving to the Cloud: Is Re-architecting Right for You?	<a href="https://www.weave.works/blog/re-architecting-move-to-cloud/">https://www.weave.works/blog/re-architecting-move-to-cloud/</a>	03/28/2017
4 Questions to Ask Before Migrating Your App or Service to the Cloud	<a href="https://www.sparkpost.com/blog/cloud-migration/">https://www.sparkpost.com/blog/cloud-migration/</a>	02/21/2018
Preparing to Adopt the Cloud: A 10-Step Cloud Migration Checklist	<a href="https://blog.newrelic.com/engineering/cloud-migration-checklist/">https://blog.newrelic.com/engineering/cloud-migration-checklist/</a>	06/04/2018
4 Reasons You Need a Privacy Policy	<a href="https://bit.ly/2H9Io49">https://bit.ly/2H9Io49</a>	02/01/2020
Front-end vs back-end vs client-side vs server-side	<a href="https://chunksofco.de/front-end-vs-back-end-vs-client-side-vs-server-side-7a04b3ec8764">https://chunksofco.de/front-end-vs-back-end-vs-client-side-vs-server-side-7a04b3ec8764</a>	11/12/2018
Upload Large Files to Amazon S3	<a href="https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/">https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/</a>	12/17/2019
AWS Lambda	<a href="https://www.amazonaws.cn/en/lambda/">https://www.amazonaws.cn/en/lambda/</a>	
AWS Security Tips	<a href="https://www.threatstack.com/blog/101-aws-security-tips-quotes-part-3-best-practices-for-using-security-groups-in-aws">https://www.threatstack.com/blog/101-aws-security-tips-quotes-part-3-best-practices-for-using-security-groups-in-aws</a>	07/03/2018
AWS Resiliency Recommendations	<a href="https://aws.amazon.com/directconnect/resiliency-recommendation/">https://aws.amazon.com/directconnect/resiliency-recommendation/</a>	
Scalability & Resilience with AWS	<a href="https://www.artifakt.io/blog/2018/01/news/cto-advice-scalability-resilience-with-aws-7599">https://www.artifakt.io/blog/2018/01/news/cto-advice-scalability-resilience-with-aws-7599</a>	01/10/2018

## Appendix F: Approvals

The undersigned acknowledge that they have reviewed the High-Level Technical Design and agree with the information presented within this document. Changes to this High-Level Technical Design will be coordinated with, and approved by, the undersigned, or their designated representatives.

Table 6 - Approvals

Document Approved By	Date Approved
----- Name: <b>Johnny Lawrence</b> , Founder – Cobra Kai	----- Date
----- Name: <b>Miguel Diaz</b> , Chief Operating Officer – Cobra Kai	----- Date
----- Name: <b>Aisha Robinson</b> , Chief Information Security Officer – Cobra Kai	----- Date
-----  Name: <b>Kevin Mukam</b> , Cybersecurity Engineer – UMD College Park	----- <b>12/18/2020</b> Date



## Appendix G: Revision History

Table 7 - Revision History

Version Number	Date	Author	Description of Change
1.0	10/22/2020	Kevin Mukam	Baseline document
2.0	12/18/2020	Kevin Mukam	Technical Plan