Cloud computing

Transitioning to a Cloud Architecture

By Salvatore, Eryk & Elvis

Contents

[Introduction: 2](#_Toc103338473)

[Executive Summary: 2](#_Toc103338474)

[Transitioning to the Cloud: 2](#_Toc103338475)

[The benefits of migrating to the Cloud: 2](#_Toc103338476)

[Scalability: 2](#_Toc103338477)

[Security: 2](#_Toc103338478)

[Cost-Efficiency: 2](#_Toc103338479)

[Abundance of additional services: 2](#_Toc103338480)

[The risks of migrating to the Cloud: 2](#_Toc103338481)

[Loss of data: 2](#_Toc103338482)

[Incompatibility of the current infrastructure: 3](#_Toc103338483)

[AWS Rekognition: 3](#_Toc103338484)

[What is AWS Rekognition? 3](#_Toc103338485)

[How will it be useful? 3](#_Toc103338486)

[Amazon RDS: 3](#_Toc103338487)

[Problem that this technology can fix: 3](#_Toc103338488)

[How to resolve this issue: 3](#_Toc103338489)

[General purpose SSD: 4](#_Toc103338490)

[Provisioned IOPS: 4](#_Toc103338491)

[Magnetic 4](#_Toc103338492)

[AWS WAF: 4](#_Toc103338493)

[Problem that this technology can fix: 4](#_Toc103338494)

[How to resolve the issue: 5](#_Toc103338495)

[Amazon EC2: 5](#_Toc103338496)

[Problem that this technology can fix: 5](#_Toc103338497)

[How to resolve the issue: 5](#_Toc103338498)

[Conclusion: 6](#_Toc103338499)

[References: 6](#_Toc103338500)

# Introduction:

## Executive Summary:

ThirdEye Pictures is a mature company which specialises in custom T-shirt printing. They wish to expand their business and upgrade their current infrastructure by transitioning towards Cloud Computing. Their current IT infrastructure is outdated, underperforming, poorly managed and vulnerable to malicious attacks due to their server instalments being integrated to their infrastructure only when necessary and not being managed by a trained professional. Additionally, there is a lack of professionalism, as the company’s backup location is in the owner’s personal residence and connected to their home internet. This document will provide an in-depth evaluation on the pros and cons of transitioning towards a Cloud based infrastructure.

# Transitioning to the Cloud:

## The benefits of migrating to the Cloud:

### Scalability:

As expressed, ThirdEye Pictures infrastructure is substandard. The scalability of their infrastructure is limited to the storage devices located in the owner’s residence, which subsequently means that it’s also poorly protected. Migrating to the cloud would eliminate the need for numerous storage arrays, as the company will be granted storage from their Cloud Service Provider. Also, this means that when ThirdEye needs to upscale, it can be done swiftly and conveniently by simply requesting it. Inadvertently, the company would also cut costs as they would only be paying for the storage they need.

### Security:

ThirdEye currently protects their data servers with FTP, a protocol that’s not built to be secure as it relies on clear-text usernames and passwords with no encryption. This means that the data is vulnerable to a variety of attacks such as sniffing, spoofing, brute force attacks, etc. The nature of the cloud means that all data backed up is encrypted and protected, which eliminates all of the vulnerabilities. The fact that Cloud Service Providers constantly analyse and update their security features means that the data is as secure as possible and will continue to be as time progresses.

### Cost-Efficiency:

The fact that the data is safely backed up online, means that ThirdEye won’t need to invest, maintain and replace any equipment in the data array. Instead, ThirdEye will simply need to pay the Cloud Service Providers for space on theirs, granting them with the privilege of investing more money and time in other aspects of the business.

### Abundance of additional services:

There is an abundance of extra services and technologies provided by AWS that ThirdEye will be able to utilise as well. These services will strengthen the current infrastructure and make it more easily manageable. The AWS technologies will be elaborated upon within this document.

## The risks of migrating to the Cloud:

### Loss of data:

Migrating the data to the cloud could result in corrupt, incomplete or missing files throughout the transfer process. This can be countered by simply creating a back-up of the data before uploading so any lost data can still be uploaded. However, ThirdEye already stores their data in offline data arrays, so in the unlikely event that any data is lost, ThirdEye will merely need to upload the missing files again.

### Incompatibility of the current infrastructure:

ThirdEye’s current infrastructure is already developed and complex. Meaning that transitioning from their current infrastructure to the Cloud could be lengthy or prone to complications. However, this can be easily avoided by seeking professional intervention for the migration process. ThirdEye should hire a team of IT experts on a short contract to; review the current infrastructure, create comprehensive documentation and guide ThirdEye through the migration process.

# AWS Rekognition:

## What is AWS Rekognition?

The company has expressed interest in integrating AWS Rekognition technology to their business model. AWS Rekognition is a deep-learning cloud-based software as a service (SaaS) that provides two API sets: one dedicated to analysing images and the other dedicated to analysing videos. Additionally, once an image/video is submitted by a user, the application stores the content’s information and provides the user with the ability to query the image/video. A plethora of reputable organizations and businesses, such as U.S Immigration and Customs enforcement (ICE) and Orlando Florida Police, have adopted AWS Rekognition due to its reliability and conventional functions.

## How will it be useful?

This powerful tool can detect objects, faces and even emotions within images and videos and can be implemented by ThirdEye Pictures to control and enhance customer experience. Once customers submit images to ThirdEye’s website, AWS Rekognition will analyse the image and detect any objects or faces and offer the client the ability to query the photo. This gives the customer the opportunity to search for any media relating to the contents of the photo submitted, e.g., a customer can submit a photo of a celebrity and be presented with the option to find other images of that celebrity, giving the customer alternative pictures to customise their product.

On the other hand, AWS Rekognition can be beneficial for ThirdEye Pictures because it can detect any hateful or violent content. If ThirdEye wishes to not perpetuate any hateful agendas or assist in hate crimes by creating negative material, then they can prevent customers from proceeding in the creation process after hateful content has been detected.

# Amazon RDS:

## Problem that this technology can fix:

ThirdEye’s current storage capabilities are not sufficient to withstand current inflow of data from customers. This problem will pose serious issues for the company as pictures send by customers are being deleted which it turns leads to unfulfilled orders and unsatisfied customers. By currents state of the storage company will have serious difficulties to attempt any further expansion on the market unless the issue is resolved.

## How to resolve this issue:

Amazon RDS offers three types of storage: gp2 (General purpose SSD), io1 (Provisioned IOPS SSD) and magnetic (also known as standard). Ech option varies from the other with performance, characteristics and price, this allows for customisability with the choice. You can choose up to 64TiB storage with instances created and ability to create a SQL server instances with up to 16TiB of storage. A simple comparison of different storage types offered by AWS to help with your choice:

### General purpose SSD:

* Baseline I/O (input, output) performance is 3 IOPS for each GiB (1 GiB = 10243 bytes) with a minimum of 100 IOPS (input/output operation per second). This suggests that the larger the volume the better the performance is. If ThirdEye is looking for storage upgrade that will require high amount of space this is the best option.
* Volumes of below 1TiB have an ability to burst to 3,000 IOPS for periods of time when the burst performance is directly linked to I/O credit.
* Gp2 is a save option as many workloads never exceed 3,000 IOPS burst storage credit, however sometimes workloads can exhaust the credit, so planning your storage capacity to meet the needs of workload is highly recommended.
* In case company chooses to go over 1TiB (maximum of 5.34 TiB) the baseline performance will be greater than burst performance, in that case burst becomes irrelevant.

In conclusion general purpose SSD is great for high volumes as the performance rises with the volume. It is recommended for a company if great storage expansion is expected.

### Provisioned IOPS:

* IO1 is for a production application that provides consistent I/O performance.
* This storage type delivers predictable performance and latency of low level.
* Drawback of this storage type is the company will be charged for the resources even when not used in a given month.
* There are options of customisability as RDS provisioned IOPS SSD storage allows for reserving I/O capacity by specifying IOPS.

In conclusion io1 is best suitable for online transactions processing workloads that require consistent performance.

### Magnetic

* Limited to maximum of 3TiB of size
* Limited to a maximum of 1,000 IOPS
* Does not support autoscaling
* Does not support elastic volumes

This type of storage is not recommended when company requires new storage, instead io1 or gp2 is recommended. Magnetic storage has backward combability but also has many drawbacks.

# AWS WAF:

## Problem that this technology can fix:

ThirdEye has experienced DDOS attacks in the past and this is to be expected especially when future expansion is planned. There are many possible weak points on website that can easily be exploited without proper security. If the problem isn't fixed and adequate security measure installed this attack will only become more frequent. Luckly there are security features that can be installed to minimalize or even totally prevent any further attacks.

## How to resolve the issue:

AWS WAF is well-rounded firewall that features many security measures that will prevent any listed issues that have already appeared as well as introduce additional security that will help with expansion. WAF offers:

* Web traffic filtering allows to filter web traffic based on conditions that include custom URLs, IP addresses and HTTP code. Firewall will also add a layer of protection against web attacks that take advantage of third-party web applications. Centralized set of rules can be deployed on mutable websites.
* Bot control allows to see and control bot traffic that can have negative affect on the website like consumption of excess resources, cause downtime or more undesired activities. There is a possibility to limit or even block bot traffic, however some of the bots are just status monitors and search engine with no malicious intent.
* Account takeover fraud prevention monitors websites login page and checks for logins using compromised credentials. Rule group to protect application from force login, stuffing attacks and other unwanted activities.
* Full feature API (Application programming interface) can be used to fully administer AWS WAF. API provides organizations that let you create and maintain rules automatically. WAF can be deployed automatically with AWS CloudFormation sample templates, this allows more control over security rules.
* Real-time visibility that in real-time show metrics and captures raw requests with detail like IP addresses, geo location, URLs. Additional feature is combability with CloudWatch that allows for setting up custom alarms when threshold is exceeded, or attacks occur. All data collected can be later used to help set up new rules for better protection.
* Integration with AWS Firewall Manager: in an instance of expansion and deploying many applications companies would be able to easily manage all the by using Firewall Manager. It automatically audits and sends alarms to security the in an instance of policy violation to help with fast response.

# Amazon EC2:

## Problem that this technology can fix:

ThirdEye has a lot of storage load issues that were causing a lot of files to get deleted, which does affect their organizational reputation. The EC2 doesn’t require maintenance due to it being a virtual server, this can potentially help ThirdEye when there is no allocated person in charge of IT, as well as help ThirdEye optimize their finances.

## How to resolve the issue:

Amazon EC2 is a virtual server, that is very efficient in terms of memory management and overall workload on the storage. Amazon EC2 offers:

* EC2 being a virtual server makes it easy to manage and does not require ThirdEye to hire hardware and maintenance specialists.
* Cost optimization greatly helps the organization to allocate its resources to the right places, EC2 makes sure the organization is only paying for what they are using, therefore saving a lot of cost for the ThirdEye organization.
* Virtual server performance can be altered, if need be, and doesn’t require any IT specialists to do so, since ThirdEye previously has issues with their systems being loaded, performance alteration will help a lot, in the end, it takes only minutes to switch.
* Instances can be hibernated if not in use, which furthermore decreases the overall costs for the EC2 virtual servers.
* Enhanced Networking allows the organization to get outstandingly swift packet per second (PPS) performance, which also includes reduced network jitter, and lower latencies.

# Conclusion:

In conclusion, migrating to a cloud infrastructure will modernize ThirdEye Pictures and improve their current business model substantially. Thanks to Cloud services and technologies, all ThirdEye’s limitations such as cost-efficiency, data security, data storage etc. will be eliminated. Additionally, the adoption of AWS Rekognition will improve the services that ThirdEye offers its customers. All around transforming ThirdEye Pictures quality.

# References:

1. Acuña, P. (2016). Amazon EC2 Container Service. In: Deploying Rails with Docker, Kubernetes and ECS. Apress, Berkeley, CA. <https://doi.org/10.1007/978-1-4842-2415-1_4>
2. Garfinkel, S., 2007. An evaluation of Amazon's grid computing services: EC2, S3, and SQS. <http://nrs.harvard.edu/urn-3:HUL.InstRepos:24829568>
3. Kareem, M., 2018. Prevention of SQL Injection Attacks using AWS WAF. <https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1094&context=msia_etds>
4. Jamal, A., Fleiner, R. and Kail, E., 2021, May. Performance Comparison between S3, HDFS and RDS storage technologies for real-time big-data applications. In *2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (pp. 000491-000496). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9465594&isnumber=9465540>
5. Hashemipour, S., Ali, M. (2020). Amazon Web Services (AWS) – An Overview of the On-Demand Cloud Computing Platform. In: Miraz, M.H., Excell, P.S., Ware, A., Soomro, S., Ali, M. (eds) Emerging Technologies in Computing. iCETiC 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 332. Springer, Cham. [https://doi.org/10.1007/978-3-030-60036-5\_3](https://doi.org/10.1007/978-3-030-60036-5_3%60)
6. Mukherjee, Sourav, Benefits of AWS in Modern Cloud (March 6, 2019). Available at SSRN: <https://ssrn.com/abstract=3415956>
7. Indla, Raghavendra Kumar, "An Overview on Amazon Rekognition Technology" (2021). Electronic Theses, Projects, and Dissertations. 1263.  
   <https://scholarworks.lib.csusb.edu/etd/1263>
8. Youssef, A.E., 2012. Exploring cloud computing services and applications. *Journal of Emerging Trends in Computing and Information Sciences*, *3*(6), pp.838-847. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.649.485&rep=rep1&type=pdf>
9. Lin, J., 2008. What is Cloud Computing. *Class lecture Presentation*. <https://cs.wmich.edu/gupta/teaching/cs6030/6030cloudFall15/lectureNotes6030cloud/cloud%20computing%20AWS,%20technical,%20parallelism%20intro.pdf>
10. S. Narula, A. Jain and Prachi, "Cloud Computing Security: Amazon Web Service," *2015 Fifth International Conference on Advanced Computing & Communication Technologies*, 2015, pp. 501-505, doi: 10.1109/ACCT.2015.20. [https://ieeexplore.ieee.org/abstract/document/7079135](https://ieeexplore.ieee.org/abstract/document/7079135’)