CAT301 Research Methods & Special Topic Study

Assignment 1: Literature Review

Security Concerns in Cloud Hosting

Teh Zhen Rong, Harold Bong Jing Choy, Muhammad Iqrar Amin, Ts. Dr. Mohd. Najwadi Yusoff zhenrong1999@student.usm.my, haroldbongjingchoy@student.usm.my, iqraramin@student.usm.my, mohdnadhir@usm.my

School of Computer Sciences, Universiti Sains Malaysia
11800 USM, Penang, Malaysia

1 Introduction

Recently, cloud computing is becoming an important platform in the modern society. It plays a vital role in enabling organizations and companies to deploy their web services without having the need to maintain and service their in-house servers. Such criterion makes this operation financially sustainable overall. The lambently debated security concerns on cloud computing has empower my team to explore current cloud securities mitigations deployed by leading companies in this field.

This report contains three sections, first section is the introduction of this report. Following that is the section 2 where we will discuss about the security concerns and how different cloud hosting platforms provide services to address these concerns. Lastly in the third section we will summarize our findings.

2 Security in Cloud Hosting Platform

In this paper my team will investigate the security vulnerability of the popular cloud platform and the current securities mitigations deployed by them. The cloud platform we choose are Azure from Microsoft, Google Cloud Platform from Google, and Amazon Web Service from Amazon. These are the leading cloud platform of the choose in Q3 2020 [1].

2.1 Azure

Azure infrastructure utilizes a defense-in-depth approach for implementing security controls in several different layers, which ranges from application security, identity and access management, data security and physical security [1]. Figure 2.1 shows few of the core security features of Azure.

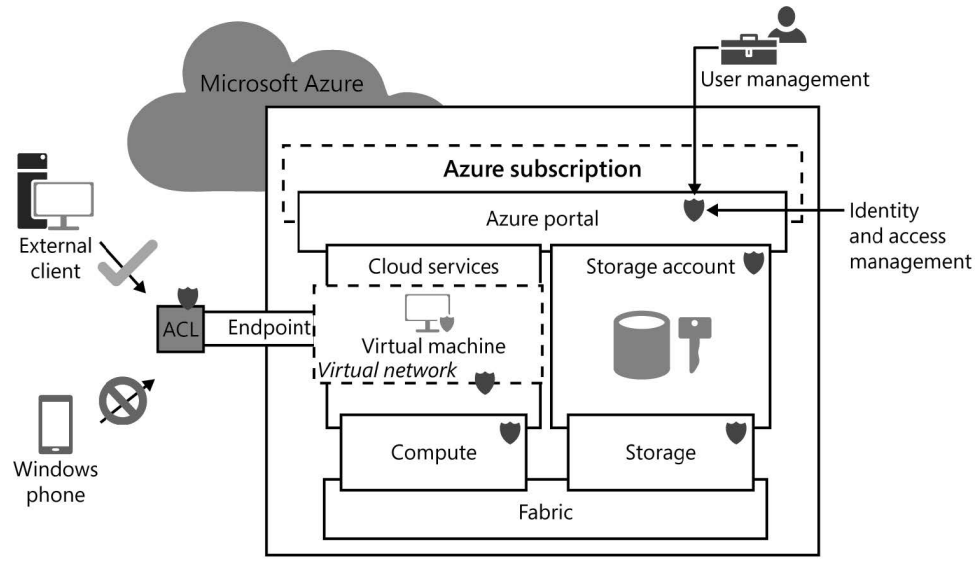

Figure 2.1: Security in Core Azure components [1]

It is also especially important to understand that when a user switch to Azure or any cloud from on-premises, where user owns the whole stack, some responsibilities transfer to Microsoft Azure. The Figure 2.2 shows the responsibility zone of the stack on-premises, software as a service (SaaS), Product as a Service (PaaS), and Infrastructure as a Service (IaaS) [2].

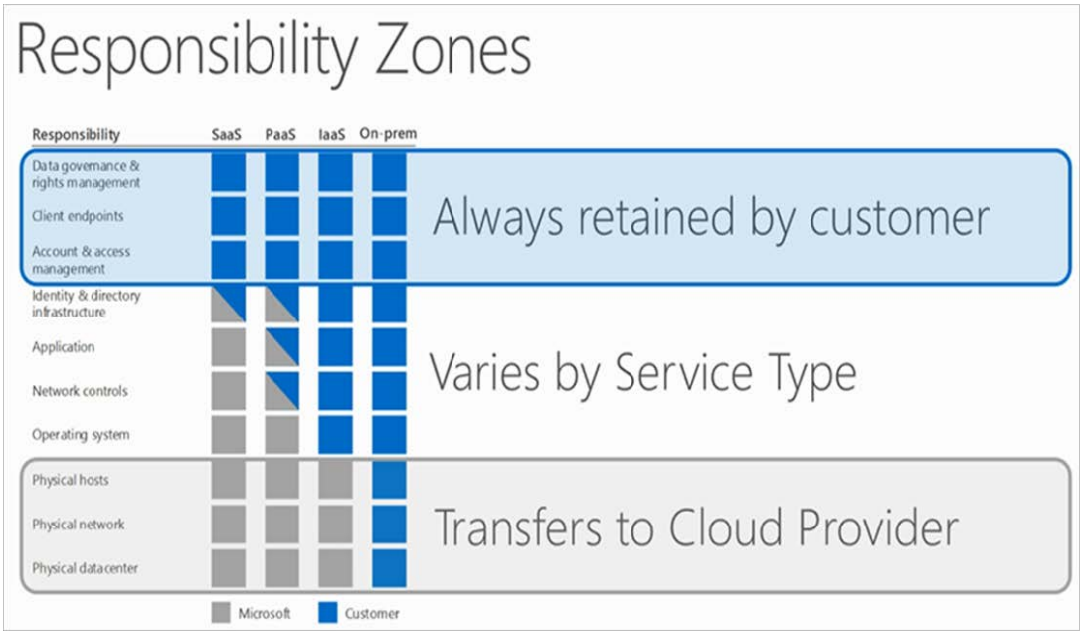

Figure 2.2: Responsibility Zone for Microsoft and Customer [2]

Azure provides number of security products that users can utilize to secure depending on their need. Azure security products include: Security Center, Key Vault, Azure DDoS Protection, and Azure Application Gateway [3]. We will investigate each of these tools one by one in the following sub sections.

2.1.1 Azure Security Center

One of the main concerns when it comes to cloud computing or hosting is the way to monitor your resources constantly to look for any threat or attack on your deployed machine, application, or service. This is especially important if users are utilizing IaaS, since they need a way to monitor network traffic, application access, and operating system management.

Azure offers its Azure Security Center which is a service that can be utilized to monitor PaaS resources like Azure SQL Database, and several Infrastructure as a Service (IaaS) resources such as Azure Virtual Machine and Azure Virtual Network [1]. It also provides protection for hybrid cloud workloads from different clouds such as AWS and GCP. This can be achieved by using Azure Defender which is integrated in Azure Security Center. It also helps user prevent, detect, and respond to threats, it also provides incremented visibility and control over the security of Azure resources [4]. The Figure shows the architecture of Azure Security Center.

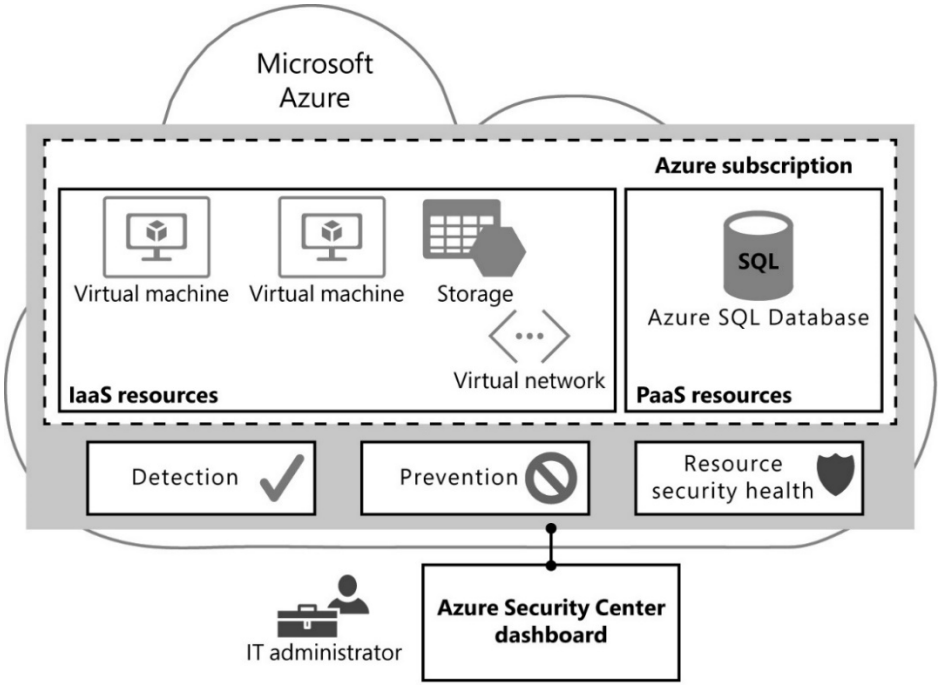

Figure 2.3: Core architecture of Azure Security Center [2]

2.1.2 Key Vault

As many organizations are moving to the cloud, they should keep control of their data's security, and one of the key element of data security is encryption. Password and key based attacks such as Brute-Force attack, Dictionary attack, Rainbow Table attack and credential stuffing, are getting popular these days and the reason behind is the easy access to the encrypted data and terrible encryption methods.

Azure tends to mitigate these risks by offering Key Vault [1], which is the cloud-based solution for some requirements for encryptions such as controlling the lifecycle of encryption keys, controlling cloud apps' keys from one place, keeping encryption keys to single region/country, keeping encryption keys to on-premises, and keeping encryption keys to dedicated HSMs. The key management mechanism is normalized by Key Vault and lets companies retain control of keys that enter and encrypt their records. Furthermore, developers can easily build keys for software creation and testing, and then move them to production keys seamlessly. The Figure 2.4 depicts the key management in Key Vault.

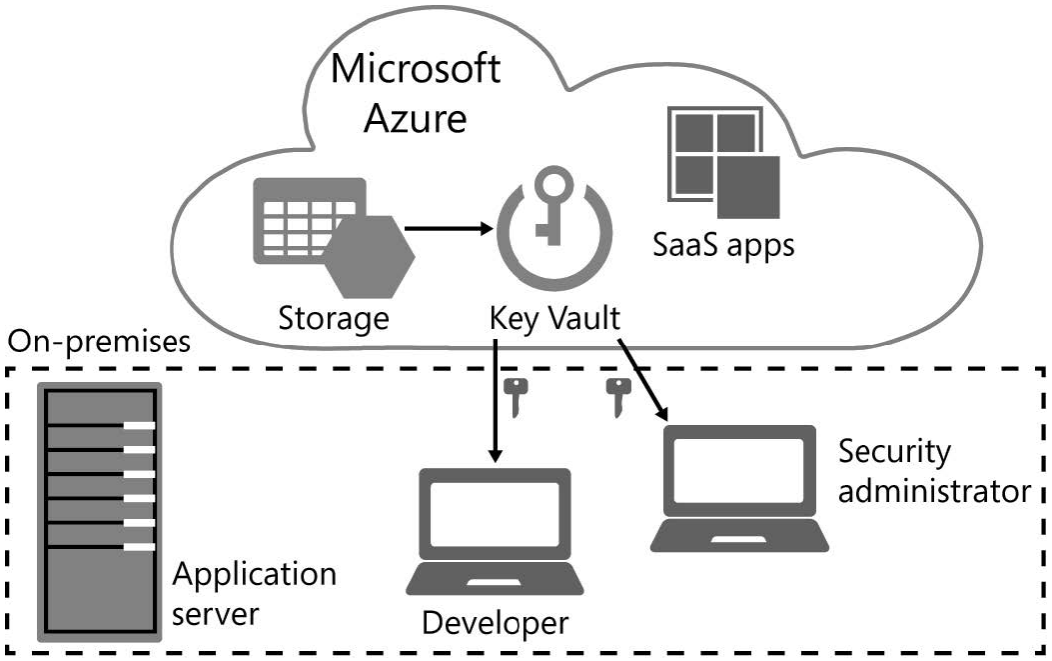

Figure 2.4: Key management using Key Vault [2]

2.1.3 Azure DDoS Protection

Distributed Denial of Service (DDoS) attack is one of the most ruinous attack and security threat which denies the services from the targeted users. The graveness of the attack depends upon the immensity of loss and duration of subsequent attack [5].

Azure has already integrated its Azure DDoS Protection (Basic) [6] in its infrastructure with no additional cost. It does not require any user configuration to provide defense against common network-based attacks. Combined with application architecture best practices, the Azure DDoS Protection (Standard) offers better DDoS mitigation capabilities to defend against DDoS attacks. To improve security of user's unique Azure assets in a virtual network, it is automatically tuned. Figure shows the difference between Basic and Standard variations of Azure DDoS Protection.

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee		●
Cost Protection		●
Mitigation policies tuned to customers application		●
Metrics & alerts		●
Mitigation reports		●
Mitigation flow logs		●
DDoS rapid response support		●

Figure 2.5: Difference between Basic and Standard DDoS Protection

2.1.4 Azure Application Gateway

Vulnerable applications can also lead to a brutal DDoS attack which could take down server for several hours. The off balancing in application network handling is the main reason for successful DDoS attacks, attacker can send huge piece of data such as images and videos which could take up all the network traffic resulting in DDoS.

Azure mitigate this risk by using The Azure Application Gateway [7], which is a network traffic load balancer that helps the web applications to handle traffic. Standard load balancers run on the transport layer (TCP and UDP OSI layer 4) and redirect traffic to the destination IP address and port depending on the source IP

address and port. The Application Gateway could make routing decisions based on additional HTTP request attributes, such as URI paths or host headers. You can redirect traffic based on the incoming URL, for instance. So, if /images is in the incoming URL, you can redirect traffic to a particular collection of image-configured servers known as a pool). If the URL is /video, the traffic is redirected to another video-optimized pool as depicted in Figure. This type of routing is known as application layer (OSI layer 7) load balancing. Azure Application Gateway can do URL-based routing and more.

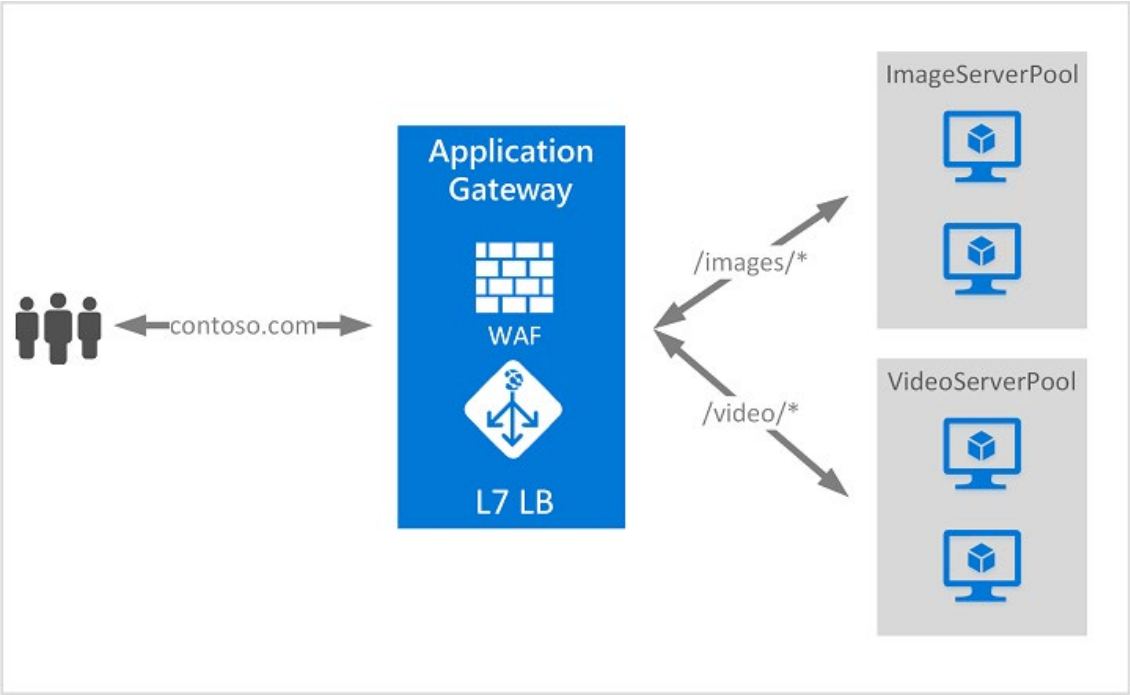

Figure 2.6: Separation of image and video-based content

2.2 Google Cloud Platform

Google Cloud Platform (GCP) is a cloud computing platform owned and maintained by Google company. Google company formally focus on search engine while nowadays Google company become a big technology company [8]. One of the goals of GCP is having Google-grade security [9] where they have proven themselves in their other applications that are used by millions of users. Same as other platforms, GCP provide SaaS, PaaS, and IaaS. Furthermore, they provide their recent technology including security used in their services to help other developers. All information

about security of cloud and handling of data is documented and listed in the online webpage.

2.2.1 Google Cloud foundation security model

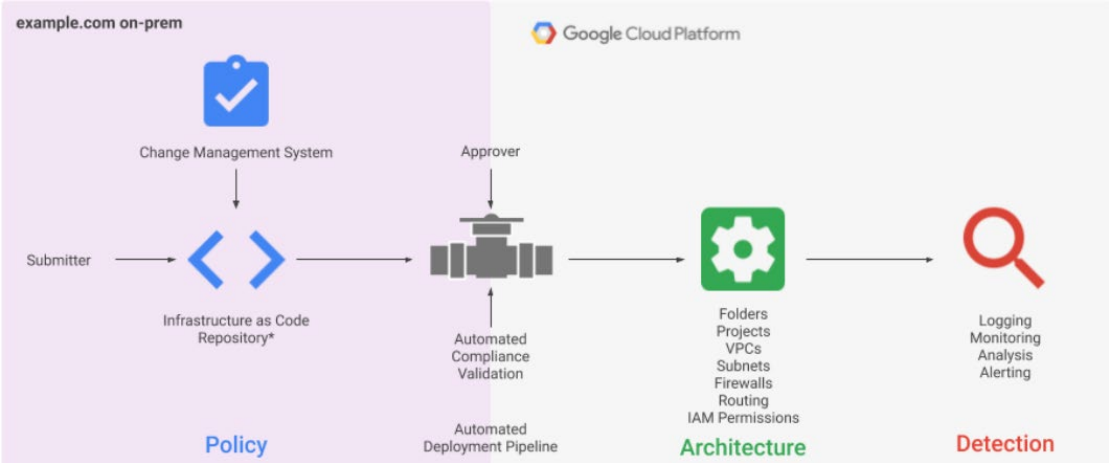

Figure 2.7: The example.com security model [10]

The foundation security of GCP is enabled through a combination of preventive control and detective control.

As shown in the figure 2.2.1 the, model consist of policy, architecture, and detection. The policy and architecture are the preventive control while the detection is the detective control

Policy is the list of steps that apply to protect organization form threats. Architecture is the infrastructure constructed and modelled in the cloud to protect the organization. Detection is a set of tools helping organization to monitor anomalous or malicious behavior.

2.2.2 Tools in GCP

As in the figure 2.2.1, our focus will be into the side of GCP where the infrastructure is given to organization to build on. In architecture, organization leverages the use of GCP services to configure their infrastructure in GCP. The tools provided are Google Cloud Identity, Google Security Manager, Google Cloud Load Balancing.

Google Cloud Identity is the tool for authentication and access management. The tool automates the maintenance of Google identities and tie their lifecycle to existing

identity management process. This heavily leverage the Google company's security on their management on the Google account that tie to GCP. The organization require to trust Google to hold the account securely which relate to Google Secret Manager.

Google Secret Manager aims to provide a secret method for storing API keys, passwords, certificates, and other sensitive data. Access to secrets is controlled through Cloud IAM and is managed individually for each organization, folder, project, or secret. This heavily leverage the Google technologies in storing sensitive data. The methods of Google storing data is based on the trust of organization to believe Google can store the data securely.

Google Cloud Load Balancing is a fully distributed, software-defined managed service. It is not hardware-based, so you do not need to manage a physical load balancing infrastructure [11]. The data transmitted using Google Cloud Load Balancing is encrypted by default [12]. This depends on Google to handle the traffics of data securely. If the tool can be trusted and used, the man in the middle attack can be reduced due to the secure in mind design of the transmitting data.

2.2.3 Google Infrastructure Security

GCP is hosted by Google company in their data centers around the world. The data center uses custom hardware and software to secure the data physically. Google's policy in building a server is not adding unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities [13]. Their servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux [13]. The hardware used is all trackable and recorded. When a storage device is retired, the storage device is erased by writing zeros to the device and performing a multiple-step verification process to ensure the drive contains no data. If the device cannot be erased for any reason, it is stored securely until it can be physically destroyed. This avoids someone recovering data from the disposal hard drive from the data center. The storage devices are all encrypted by leveraging technology like FDE (full disk encryption) and drive locking, to protect data at rest [13].

Google company also invests a lot in protecting their employees' devices and credentials from compromise and in monitoring activity to discover potential

compromises or illicit insider activity [14]. Google company aggressively limit and actively monitor the activities of employees who have been granted administrative access to the infrastructure and continually work to eliminate the need for privileged access for tasks by providing automation that can accomplish the same tasks in a safe and controlled way [14]. Both reduces the risk of leakage from the operational level of maintain GCP services by the company's employees.

2.3 Amazon Web Services

Amazon Web Services (AWS) is a cloud computing platform with over 175 products specialized in various fields such as data analytics, quantum technologies etc. AWS, as what other popular platforms provides, aims to reduce cost, and increase efficiency of users' products. Amazon reported AWS revenue of $11.6 billion (about $36 per person in the US) for Q3 2020 which grew 29% compared to the previous year, holding 32% of the market and generated more revenue than Microsoft Azure (19%), Google Cloud (7%) and Alibaba Cloud (6%) combined [14].

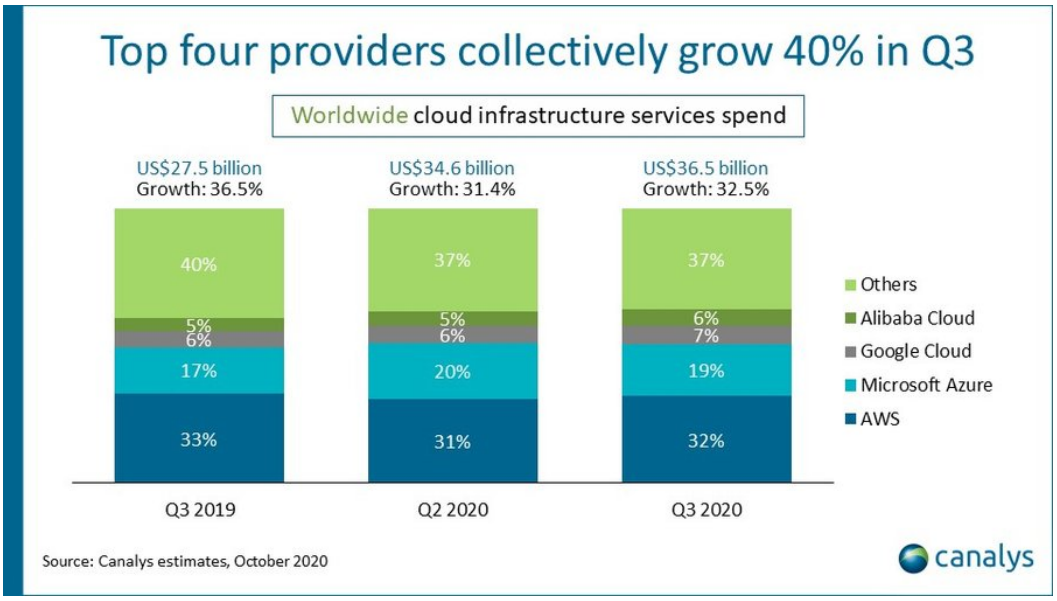

Figure 2.8 : Cloud Computing Market Share Breakdown [14]

2.3.1 Amazon Elastic Compute Cloud

Amazon Elastic Compute Cloud (Amazon EC2) is a web service with computing scalability to give easier control for developers to control the web computing power [15]. Amazon EC2 web service port can retrieve and receive storage easily and everything can be managed in this AWS environment. Though scalability is a great

approach for better resource management, it also increases the exposure to **potential attacks** from third parties especially DDoS attacks.

AWS Shield is built upon DDOS resiliency practices to protect applications running in AWS. It provides continuous detection and automatic inline mitigation function to reduce application shutdown time and delay. All AWS users are free to use AWS Shield Standard to protect their applications from most of the DDoS attacks that target websites or applications. For important and sensitives applications which is running on resources like Amazon Elastic Compute Cloud (EC2) or Elastic Load Balancing (ELB), AWS Shield provides higher security by introducing the Advanced level [16].

A few resiliencies have been introduced to overcome DDoS attacks. Below here are three examples [17].

1 Choice of Region - international carriers and large peers have a strong presence can help the internet capacity to mitigate larger attacks.
2 Elastic Load Balancing (BP6) - distributing internet traffic to multiple backend created instances to reduce the risk of overloading.
3 Domain Name Resolution at the Edge (BP3) – lets users access your application even if the DNS service is targeted by a DDoS attack by shuffle sharding and anycast striping.

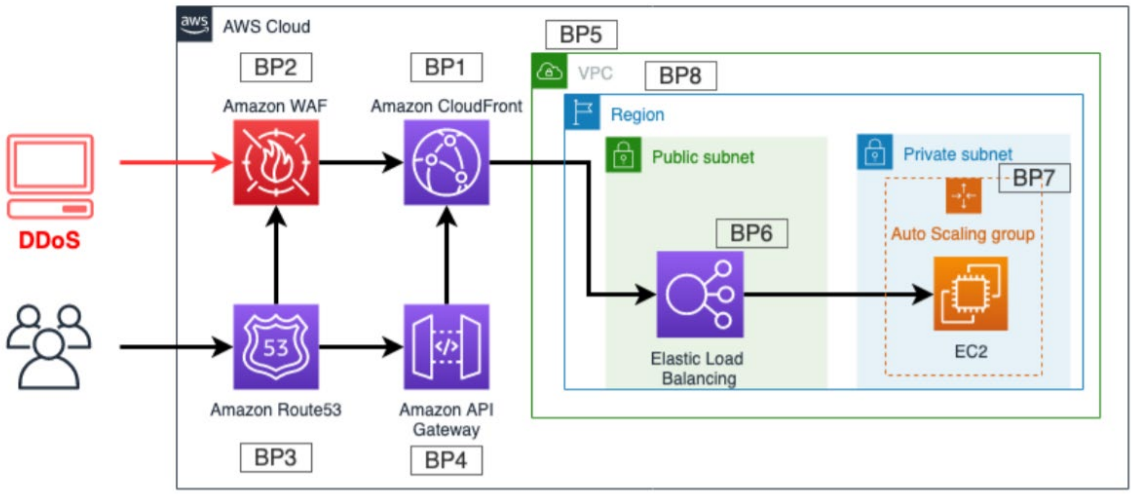

Figure 2.9: DDoS-resilient reference architecture [17]

2.3.2 AWS Identity & Access Management (IAM)

IAM enables you to securely manage access to AWS services and resources. Users can use IAM to create and manage AWS users and groups and use various permissions to allow or deny their access to AWS resources [18]. However here imposes a risk where individuals who gained access to the resources can control it without head user notice. Failing to assess, track and inspect all type of unauthorized access to resources is one of the reasons for insider leaks and data breaches. The issue becomes difficult to solve over time, as companies add new services to their IT infrastructure without developing the capability to review, audit and track their access provisioning and de-provisioning process.

Since this is hard to prevent on infrastructure level, Amazon released a guideline on AWS security audit especially in IAM field. Some of the advices are below [19]:

1 Lists out active users and inactive users on IAM and remove users that are not relevant.
2 Review periodically security policies of groups that users are in and delete the security credentials that have been exposed or outdated.
3 Always review the permission granted to users according to their role and level of trust.

2.3.3 Data Classification

AWS dedicated database product supports a variety of data models, allowing you to build distributed applications that are driven by use cases and are highly scalable. By choosing the most suitable database to solve a specific problem or set of problems, you can get rid of the general large database with many limitations and focus on building applications to meet business needs. Having sensitive data storing on these models has risks if any unintended or unauthorized users gain the access to it. An organization may have many projects but not all employees need to access all database for project developments. Hence, Amazon introduce Amazon VPC to launch AWS resources into a virtual network with the advantages of utilizing the flexible architecture of AWS, this virtual network closely resembles a conventional network that you can run in organization own data center [20].

Some of the key concepts of Amazon VPC [20]:

1 Subnet - A range of authorized IP addresses in your VPC group.
2 Route table - A set of rules (routes) used to determine where network traffic is directed.
3 Internet gateway - A gateway that attached to your VPC to enable communication between resources in your VPC and the internet.

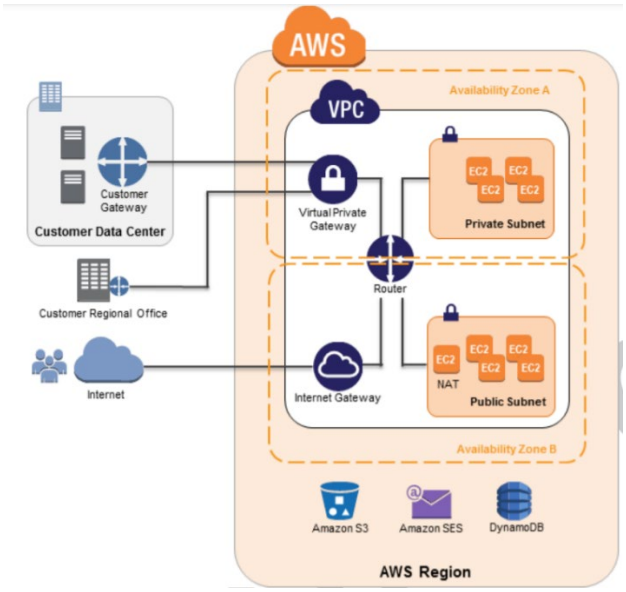

Figure 2.10: Amazon VPC Architecture [17]

3 Summary and Future Work

The three companies we reviewed have some similarity in features and security measures in place (such as data protection, DDoS protection, and access management) when providing cloud platform. Although they publish their security documents publicly for their users to evaluate and ensure that their platform is safe to use, there are still some unknown security features that are transparent to users such as the underlying technology in securing and transmitting their data. This transparency invoke the questions about trust and privacy of data towards the cloud providers that we reviewed. Moreover, there is also transparency in the technologies that are being used in cloud computing, there are a lot of hidden technologies used under the hood that users are unaware of and they have to rely on cloud providers to protect their data.

This review also lays the ground for future work on the literature where one can emphasis on those hidden/transparent technologies or services provided by cloud hosting platforms. There is also a need for more third-party trustable reviewer to review the security of the cloud platform provided.

4 References

[1] Y. Diogenes, D. T. W. Shinder and D. L. Shinder, Cloud Security Considrations, Microsoft Azure, 2016, p. 15.

[2] M. Corporation, "Security best practices for Azure solutions," Microsoft Corporation, 2018.

[3] Microsoft, "Security," Microsoft Azure, 2020. [Online]. Available: https://azure.microsoft.com/en-us/product-categories/security/#:~:text=Protect%20data%2C%20apps%2C%20and%20infrastructure,data%2C%20hosts%2C%20and%20networks.. [Accessed 20 11 2020].

[4] Microsoft, "Azure Security Center," Microsoft Azure, 2020. [Online]. Available: https://azure.microsoft.com/en-us/services/security-center/. [Accessed 20 11 2020].

[5] Vanitha.K.S, D. V. UMA and Mahidhar.S.K, "Distributed Denial of Service: Attack techniques and mitigation," in *Proceeding of Second International conference on Circuits, Controls and Communications*, 2017.

[6] Microsoft, "Azure DDoS Protection Standard overview," 09 09 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview. [Accessed 20 11 2020].

[7] Microsoft, "What is Azure Application Gateway?," 26 08 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/application-gateway/overview. [Accessed 20 11 2020].

[8] Google, Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Google. [Accessed 20 11 2020].

[9] Google, "What makes Google Cloud Platform different?," Goolge, [Online]. Available: https://cloud.google.com/free/docs/what-makes-google-cloud-platform-different. [Accessed 20 11 2020].

[10] G. C. Whitepaper, "Google Cloud security foundations guide," August, 2020..

[11] "Cloud Load Balancing overview | Google Cloud.," [Online]. Available: https://cloud.google.com/load-balancing/docs/load-balancing-overview. [Accessed 20 11 2020].

[12] "Encryption in Transit in Google Cloud,," [Online]. Available: https://cloud.google.com/security/encryption-in-transit/#authentication_integrity_and_encryption. [Accessed 20 11 2020].

[13] G. C. Whitepaper, "Google security whitepaper," January 2019. [Online]. Available: https://services.google.com/fh/files/misc/google_security_wp.pdf. [Accessed 20 11 2020].

[14] "AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows," Katy Stalcup, 12 November 2020. [Online]. Available: https://www.parkmycloud.com/blog/aws-vs-azure-vs-google-cloud-market-share/. [Accessed 17 November 2020].

[15] "Amazon EC2," Amazon Web Services, Inc, [Online]. Available: https://aws.amazon.com/cn/ec2/?ec2-whats-new.sort-by=item.additionalFields.postDateTime&ec2-whats-new.sort-order=desc. [Accessed 17 November 2020].

[16] "Amazon Field," Amazon Web Services, Inc, [Online]. Available: https://aws.amazon.com/cn/shield/. [Accessed 17 November 2020].

[17] "AWS Best Practices for DDoS," Amazon Web Services, Inc, December 2019.

[Online]. Available: https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf. [Accessed 17 November 2020].

[18] "AWS Identity and Access Management (IAM)," Amazon Web Services, Inc, [Online]. Available: https://aws.amazon.com/cn/iam/. [Accessed 17 November 2020].

[19] "Security best practices in IAM," Amazon Web Services, Inc, [Online]. Available: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html. [Accessed 17 November 2020].

[20] "What is Amazon VPC?," Amazon Web Services, Inc, [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html. [Accessed 17 November 2020].

[21] W. G. C., "Google Cloud security foundations guide," 2020.