International Journal of Advanced Trends in Computer Applications
www.ijatca.com

EVALUATION OF SECURITY IN CLOUD SERVICE PROVIDERS

[1]**Folorunso Olufemi Ayinde** *Ph.D,* [2]**Alebiosu Omobolade B.**
[1]Folorunso Olufemi Ayinde *Ph.D*
Wellspring University, Benin City, Edo State, Nigeria
[2]Alebiosu Omobolade B.
National Open University of Nigeria
[1]dict@wellspringuni.edu.ng, [2]boladealeb@gmail.com

ABSTRACT: *The recent influx in the deployment of cloud computing can be attributed to large, medium, small enterprises and individuals' quest to decrease IT cost and overcome economic recession. However, the cloud is still faced with challenges such as data breaches, data loss, malicious insider and denial of service attacks and all point to security of the cloud. This makes security an important discuss in cloud computing, which led to the objectives of this research, which are toevaluate security protocols or measures employed by major cloud service providers and offer recommendations to both Cloud Service Providers (CSPs) and the user.The research employed comparing techniques to evaluate the security measures and protocols employed by the top three cloud service providers which are Microsoft, Amazon and Google. It is worthy to note that, the compute service of CSPs are claimed to be secured as well as their storage services. It is recommended that CSPs provide a 2-factor authentication for users, this ensures that cloud users use very strong password or keys. While cloud users should ensure proper cloud logging and authentication, they should also avoid weak and generic passwords, as weak and generic password makes the cloud susceptible to breaches.*

Keywords: Cloud, Computer Security, Cloud Service Provider, Amazon, Microsoft, Google.

I. INTRODUCTION

The recent influx in the deployment of cloud computing can be attributed to large, medium, small enterprises and individuals' quest

to decrease IT cost and overcome economic recession. The high demand can also be attributed to characteristics of cloud computing which are; it gives users ability to access the service through several platforms such desktop computers, mobile phones, laptops. Etc, it gives users the ability to pool resources simultaneously, it has the capability to withstand high demands and the cloud computing paradigm allows people to only pay for services used without cost of purchasing physical hardware. Furthermore, IT trends have set a standard and somewhat determined how cloud computing is developed. It is efficient and cost economical for consumers to use computing resources as much as they need or use services, they require from cloud computing provider, and moving data into the cloud is easier than the grid computing format, as users and organizations need not to worry about the complexities of direct hardware management as clouding computing offers great convenience.

Additionally, other computing services have been abashed by recent spotlight on Cloud Computing this is due to the huge capacity and unlimited amount of resources the cloud provides. Folorunsoopined that the cloud computing models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), gives users several advantages such as cost effectiveness, efficient resource utilisation, collaboration, disaster recovery and high performance [1]. However, Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers, and most often System administrators potentially can become attackers.

1.1 Description of Top 3 CSPs

Amazon has a long history of using a decentralized IT infrastructure. This arrangement enabled their development teams to access, compute and store resources on demand, and it has increased overall productivity and agility. The AWS was launched by Amazon in other to help organizations benefit from Amazon’s investment in running large-scale distributed, transactional IT infrastructure as well as its experience [2]. While, Microsoft has deployed many Azure datacentres around the globe, with more planned. Additionally, Microsoft is increasing sovereign clouds in regions like China and Germany. Only the largest global enterprises can deploy datacentres in this manner, so using Azure makes it easy for enterprises of any size to deploy their services close to their customers [3]. And Google today plays a central in the branch of Cloud Computing which is defined as a technique of providing the services through the Internet with the capabilities to accommodate user requirements. Through Google’s API service platform, possibilities are offered to the developer’s community and the companies to develop and host their web-based applications.

II. RESEARCH METHODOLOGY

This study employed comparing techniques in order to evaluate the security measures and protocols employed by the top three cloud service providers which are Microsoft, Amazon and Google are features and parameters.

Features used in differentiating cloud service providers are compute, file storage, pricing, databases, security, policies, revenue and market share. While the parameter used in comparing the three cloud service providers are data protection or security, infrastructure security and privacy.

2.1 DESCRIPTION OF FEATURES AND PARAMETERS

2.1.1 Features for Comparison

Compute: Compute is used to describe concepts and objects which are geared towards computation and processing in cloud computing it also refers to activities, applications and workload that require processing resources than its regular resource requirements [4].

File storage: Storage in cloud is a method of storing data, it provides servers and applications access to data through shared file systems. Cloud service providers provide a range of different storage options such as object storage, block storage, archive storage, backup etc.

Pricing: Comparing the cost between AWS, Azure and Google Cloud could be difficult as each provider updates their pricing model multiple times a year. This is as a result of the brooding competition.

Databases: The expansive storage capabilities cloud computing provides is regarded as one of the greatest advantages of cloud computing. Databases in cloud computing are as it is with normal IT operations.

Security: Security is regarded as an essential feature of cloud computing, as it ensures the safety of data, by creating a snapshot of the data stored so that the so that data loss is prevented in case of eventualities [5].

Policies: Policies such as Data Loss Prevention (DLP) Policies are emplaced as a process for protecting sensitive data and confidential information at rest, in transit, and on endpoints to reduce to reduce the likelihood of data theft or unauthorized exposure [6].

Revenue and market share: Economic Times defined market share as the percentage that goes to a company out of the total purchases of a customer of a product or service and in this case cloud computing.

2.1.2 Parameters for Comparison

Infrastructure Security: This could also be regarded as authentication and identity, which involves multi-factor authentication, addressing anonymous use, enterprise identity etc. as well as avoiding abnormal behavior of ports by scanning them and ensuring security patches are updated as soon as possible [7].

Privacy: Encrypting data, controlling user privileges, etc. However, cloud providers have little control over this, has this is usually the user's responsibilities.

Data Security or Protection: This research seeks to establish what your data security goals should be, while comparing the security measures each provider employs to protect your data as individuals also understand their own part in data security.

2.1.3 Other Comparison Tool

Google Trends: Google Trends shows how often a particular search term is entered using the public web facility of Google Inc., based on Google Search, it shows the data in relation to the total search-volume across various regions of the world, and in various languages [8].

III. RESULTS AND DISCUSSIONS

3.1 Features for Comparison

3.1.1 Compute

Table 1: Compute of Top 3 CSPs.

AWS	Microsoft Azure	Google Cloud
Elastic Compute Cloud: EC2 is Amazon's flagship compute service. The EC2 is a web service that provides a compute which is secure and resizable in the cloud. It offers a variety of options, support for Windows and Linux [9].	**Virtual Machines:** The primary compute service of Microsoft is simply known as virtual machines. Which supports Linux, Windows Server, SQL server, Oracle, IBM and SAP, as well as enhanced security, hybrid cloud capabilities and integrated support for Microsoft software.	**Compute Engine:** The primary compute service is called Compute Engine. It offers support for both windows and Linux, at a per second billing rate, automatic discounts as well as carbon-neutral that uses half of the energy of a typical data centre. While also providing custom and predefined machine types [10].
Container Services: Various container services are increasing in popularity in the compute category. With options that support Docker, Kubernetes, and Amazon's Fargate Services that automates server and cluster management when using containers. As well as offering virtual private cloud options.	**Additional Services:** Virtual Machine Scale Sets is Microsoft Azure version of Auto Scaling. This has two container services: Azure container service which is based on Kubernetes and uses Docker Hub, and Amazon Container Registry for management. Service Fabric is one of it unique offering, which is specifically designed for applications with microservices architecture.	**Focus on Kubernetes:** Google also offers Kubernetes Engine for organisations interested in deploying containers. Like all of the leading cloud vendors, it offers containers and microservices.

3.1.2 Storage and Database

Table 2: Storage of Top 3 CSPs.

	AWS	Microsoft Azure	Google Cloud
File, object, Block, Archive Storage	AWS offers a long list of storage services that includes its Simple Storage Service (S3) for object storage, Elastic Block Storage (EBS) for persistent block storage,	The basic storage service of Microsoft Azure's includes Blob Storage, Blobs are basically files, which uses a Data Lake Store for big data applications.Queue Storage for large-volume workloads,	The GCP has a smaller menu of storage services available. The unified object storage service of the GCP is the Cloud Storage, it has

	and Elastic File System (EFS) for file storage. Storage Gateway and Snowball are some of AWS innovative storage products.the Storage Gateway enables hybrid storage environment, while Snowball enables a physical hardware device that organizations can use to transfer big data in circumstances where transferring it over the internet is not feasible.	File Storage and Disk Storage all use the REST-based object storage (Blob) which are unstructured data [10].	a persistent disk option, while offering a transfer appliance which is similar to AWS Snowball, as well as online transfer services[11].
Database	AWS has a SQL-compatible database called Aurora, Relational Database Service (RDS), DynamoDB NoSQL database, Elastic Cache in-memory data store, Redshift data warehouse, Neptune graph database and a Database Migration Service. In addition, its Storage Gateway can be used to easily set up backup and archive processes.	Azure has three SQL-based options: SQL Database, Database for MySQL and Database for PostgreSQL. The in-memory service is Redis Cache and its hybrid storage service which is designed specifically for organizations that use Microsoft SQL server in their data centres is the Server Stretch Database.	The Cloud Spanner is designed for mission-critical workloads in GCP, it is the SQL-based Cloud SQL and a relational database. Its two NoSQL options are: Cloud Bigtable and Cloud Datastore. It does not have backup and archive services [12].
Disaster and Recovery	Disaster Recovery	Disaster Recovery	Site Recovery

3.1.3 Pricing, Revenue and Market Share

Table 3: Pricing and Revenue of Top 3 CSPs.

	AWS	**Microsoft Azure**	**Google Cloud**
Revenue	$9.94 billion 34% growth in fourth quarter (Q4) of 2019.	$11.9 billion 27% growth in Q4 2019.	$2.6 billion 53% growth from the previous year.
Upfront Payment	Yes	Yes	No
Partial Upfront	Yes	No	No
Flexibility	Convertible: can be exchanged for reserved instances of greater or equal value.	Can be exchanged for other reserved instances.	Automatically applies to all instances in the region.
Length of Commitment	Reserved instance: 1 or 3 years.	Reserved VM instance: 1 or 3 years	Committed use discounts: 1 or 3 years.

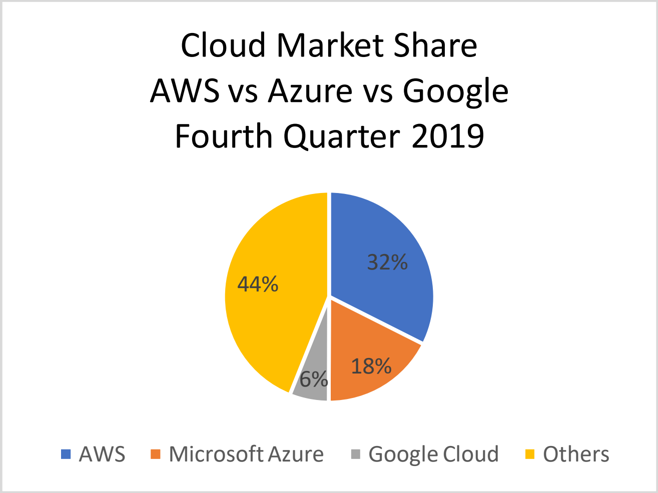

Figure 1: Market Share of CSPs.

3.2 SECURITY

The Shared Responsibility Model, is the best way to ensure optimal security of the cloud, as all organizations that use cloud computing need to be vigilant in doing their due diligence, regardless of the effortsof cloud service providers [7].

3.2.1 AWS Cloud Security

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data centre and network architecture built to meet the requirements of the most security-sensitive organizations. Two of the best AWS security features are their excellent implementation of security groups (firewalls) and granular IAM.

3.2.2 Microsoft Azure Cloud Security

Azure stated that, 8 trillion threat signals are analysed daily, thereby deploying cloud and large-scale intelligence decades of Microsoft security experience to work. Making your threat detection and response smarter and faster with AI-driven security signals that modernize your security operations [13].

Google Cloud Security

States that security drives their organizational structure, training priorities and hiring processes. As it also shapes the way they deploy the technology they house and theirdatacentres. It's central to our everyday operations and disaster planning, including how we address threats.

3.3 Result of The Parameter

Table 4: Parameter: AWS vs Azure vs Google Cloud

Parameter	**AWS**	**AZURE**	**GOOGLE CLOUD**
Data Security	AWS key management service, AWS cloud Hardware Security Module (HSM) – allows users generate their own encryption keys, AWS Market Place Solution – allows third party vendor solution, bring your own encryption solution – allows users with existing on-premise encryption solution deploy it on the cloud.	Azure Key Vault – helps safeguard cryptographic keys and secrets that cloud application use, Azure Information Protection – is a cloud-based solution that helps organisations classify and protect documents, data loss prevention (DLP) policy - it identifies, monitors and protect sensitive information.	Google cloud automatically encrypts data which is accessed only by authorized roles or audited services which have audited access to encryption keys, cloud key management system (KMS), cloud HSM and DLP. Which is an in-built data protection solution.
Infrastructure Security	Defines user permissions and identities, infrastructure protection for a smooth AWS adoption strategy.	Employs security defaults to help protect the organization from attacks using preconfigured security settings.	Compute engine persistent disks are encrypted at rest using keys protected by central infrastructure key management system.
Privacy, Authentication and Authorization	Identity and Access Manager (IAM), Multi-factor AWS Authentication (MFA), Federated Identity, Access keys and Key pairs.	Data encryption at rest – a mandatory step towards data privacy, Azure Active Directory	Gooogle Cloud Identity and Access Manager (IAM), end user authentication to the compute engineis done via Google's centralized identity service.
Policies	Automated incident response and recovery to help shift the primary focus of security teams from response to analysing root cause and resource-based policies for permission management.	Unified multi-factor authentication registration, create custom security policies, Azure policy.	Google Cloud Armor Security Policies.
Firewalls	Security groups, AWS web application firewall	Azure Firewall (Endpoints only), Azure application gateway	Firewall rules using tags, VPC firewall rules, hierarchical firewall policies.
Shared Network Cloud	Yes	No	No
Virtual Private Cloud Network	Yes	Yes	Yes
Secure extension using IPsec	Yes	Yes	Only in Beta
Remote access to cloud servers	SSH/RDP	SSH/RDP	SSH/RDP
VPN access	No	Yes	No
Threat detection and	Amazon guard duty	Azure security and compliance	Cloud Armor (Beta)

monitoring			

3.4 Google Trends

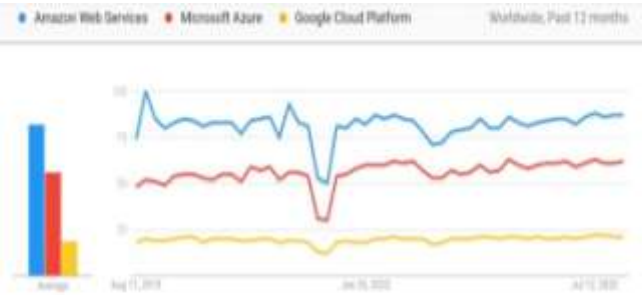

Figure 2: Google Trends on AWS, Azure and Google Cloud

IV. CONCLUSION

It is evident from this project work that Amazon, Microsoft and Google are the top 3 CSPs, as they hold the largest segment of the market share, this implies that they are the most used CSPs. Amazon has an aging history of decentralized IT infrastructure, and poses a low-cost entry point which is affordable by small businesses while Google offers a technique flexible to accommodate user requirements. Additionally, these CSPs compute service which is claimed to be secured as well as a variety of storage services, similar database services while they all promise recovery in case of a disaster.

Furthermore, security is said to be the highest priority for Amazon, Amazon equally claims that their cloud security is similar to on-premise computing security, as they have pre-installed software-based security tools with adequate support. Additionally, Microsoft has spent $1B+ on investment in security research and development, equally employed 3500 cybersecurity experts whose tasks are to protect business data. It becomes pertinent to state that, all 3 CSPs have in-built security measures and several security techniques to enhance data security as well as data loss prevention policy.

V. RECOMMENDATIONS

The research findings showed that cloud service providers have a commendable level of security pre-installed, security software and measures available on demand while leaving the rest of the work to user to prevent insider sabotage or prevent using of weak or generic passwords, as the make it easy for the cloud to be breached. To this end my recommendations are directed at the main dwellers of cloud computing which are the cloud service providers (CSPs) and the cloud users.

CSPs should continually budget for security research and development, as the field of Information Technology is an ever-evolving field, this would help continually improve the security of the underlying infrastructure of their cloud service, because most inhibitors of cloud adoption is security and privacy issues, Additionally, cloud service providers should provide a 2-factor authentication for users, this ensures that cloud users use very strong password or keys.

Cloud Users which includes the individual users, academia, medium scale enterprises and corporate organisations, should ensure proper cloud logging and authentication, this puts control to who has access to what on the cloud and this in turns the risk of internal security breach, as a breach could easily be traced to those who have access to the cloud. Cloud users should also avoid weak and generic passwords, as weak and generic password makes the cloud susceptible to breaches.

VI. FUTURE WORK

In our future work, we hope to have data samples for in-depth analysis into the security state of CSPs while also evaluating all CSPs using redefined parameters.

REFERENCES

[1] Folorunso et al — Evaluation of Cloud Computing Model: Software as a Service (SaaS) and Platform as a Service (PaaS), International Journal of Advanced

Research in Computer Science and Software Engineering Vol. 5, Issue 12, pp 140-149, December 2015.

[2] Jinesh Varia and Sajee Mathew — Overview of Amazon Web Service, Amazon Web Service, January 2014.

[3] Microsoft – Get Started for Azure IT Operators, accessed 2March 2020 on24 August 2018

[4] Techopedia - Compute, accessed 29 June 2020 on27 December 2016

[5] RinuGour – 9 Major Characteristics of Cloud Computing, DZone, accessed 29 June 2020 on, January 2019.

[6] Nate Lord – What is Cloud DLP, Digital Guardian, accessed 29 June 2020 on , September 2018.

[7] The State of Security -AWS vs. Azure vs. Google – What’s the Difference from a Cloud Security Standpoint? accessed 30 June 2020 on, 29 December 2019.

[8] IGI Global – What is Google Trends, accessed 29 June 2020.

[9] Fandom – Identify the core AWS services, accessed 30 June 2020 .

[10] Rightcloud– AWS V/S Microsoft Azure V/S Google Cloud, accessed 30 June 2020, 22 August 2018.

[11] CliffAffairTechnologie - AWS vs. Azure vs. Google: Storage, accessed 30 June 2020.

[12] Datamation – AWS vs. Azure vs. Google: 2020 Cloud Comparison, accessed 30 June 2020 on 17 March 2020.

[13] Microsoft Azure – Trust your cloud, accessed 30 June 2020.