A Perspective View of Amazon Web Services with Respect to Security Issues

[1]Dr.M.Thillainayaki, [2]Ms.S.Sabeena, [3]Ms.R.Mahadevi, [4]Ms.N.Saranya

Assistant Professor, [1,2,4]Department of Computer Science, [3]Department of Commerce, Nehru Arts and Science College, Coimbatore, India.

[1]thillainayakim@gmail.com, [2]sabeena.mphil@gmail.com, [3]mahadevi.ramasamy@gmail.com, [4]nsaranyanatraj@gmail.com

Abstract -Amazon Web Services (AWS) presents many benefits, such as increased business liveliness and adaptability, as well as cost reduction. In order to realize the benefits, environment needs to require new skills and manipulating the important processes. The business value can be maximized and minimizing the risks of business in a cloud environment. The AWS Cloud Adoption Framework (AWS CAF) helps organizations determines how cloud could adopt the transformations the way that works, and provides the structure to identify the gaps, which it addresses and processes easily. Helping to preserve the security, integrity and availability of our customer's systems and data is of the utmost importance to AWS, as is preserving customer trust and confidence. This system leverages our insights and best practices in helping organizations around the world navigate their journey through cloud adoption.

Keywords: Amazon Web Services(AWS), Platform, Security

I. INTRODUCTION

At the AWS CAF organizes feedback at the highest level into six focus areas. We define such areas of focus as Perspectives. Figure 1 displays the CAF's six AWS Perspectives.

In general, the Business, People, and Governance Perspectives specialize in business capabilities, and therefore the Platform, Security, and Operations Perspectives specialize in technical capabilities.

• **Business Perspective –** Common roles: Business Managers, Finance Managers, Budget Owners, and Strategy Stakeholders. Helps stakeholders understand the way to update the staff skills and organizational processes they're going to got to optimize business value as they move their operations to the cloud.

• **People Perspective –** Common roles: Human Resources, Staffing, and People Managers. Provides guidance for stakeholders liable for people development, training, and communications. Helps stakeholders understand how to update the staff skills and organizational processes they will use to optimize and maintain their workforce, and ensure competencies are in place at the appropriate time.

• **Governance Perspective –** Common roles: CIO, Program Managers, Project Managers, Enterprise Architects, Business Analysts, and Portfolio Managers. Provides guidance for stakeholders liable for supporting business processes with technology. Helps stakeholders understand the way to update the staff skills and organizational processes that are necessary to make sure business governance within the cloud, and manage and measure cloud investments to evaluate their business outcomes.

• **Platform Perspective –** Common roles: CTO, IT Managers, and Solution Architects. Helps stakeholders understand the way to update the staff skills and organizational processes that are necessary to deliver and optimize cloud solutions and services.

• **Security Perspective –** Common roles: CISO, IT Security Managers, and IT Security Analysts. Helps stakeholders understand the way to update the staff skills and organizational processes that are necessary to make sure that the architecture deployed within the cloud aligns to the organization’s security control requirements, resiliency, and compliance requirements.

• **Operations Perspective –** Common roles: IT Operations Managers and IT Support Managers. Helps stakeholders understand the way to update the staff skills and organizational processes that are necessary to make sure system health and reliability during the move of operations to the cloud and then to work using agile, ongoing, cloud computing best practices.

In a transition to the cloud, stakeholders need to participate and actively support organizational and operational change for their region within each AWS CAF Perspective.

DOI : 10.35291/2454-9150.2020.0073

The AWS Well-Architected Framework is predicated on five pillars — operational excellence, security, reliability, performance efficiency, and price optimization.

The Well-Architected Framework identifies a group of general design principles to facilitate good design within the cloud:

• **Stop guessing your capacity needs:** Eliminate guessing about your infrastructure capacity needs. When you make a capacity decision before you deploy a system, you would possibly find yourself sitting on expensive idle resources or handling the performance implications of limited capacity. With cloud computing, these problems can go away. You can use the maximum amount or as little capacity as you would like , and proportion and down automatically.

• **Test systems at production scale**: In the cloud, you can create a production-scale test environment on demand, complete your testing, and then decommission the resources. Because you only pay for the test environment when it's running, you can simulate your live environment for a fraction of the cost of testing on premises.

• **Automate to make architectural experimentation easier**: Automation allows you to create and replicate your systems at low cost and avoid the expense of manual effort. You can track changes to your automation, audit the impact, and revert to previous parameters when necessary.

• **Allow for evolutionary architectures**: Allow for evolutionary architectures. In a traditional environment, architectural decisions are often implemented as static, one-time events, with a few major versions of a system during its lifetime. As a business and its context continue to change, these initial decisions might hinder the system's ability to deliver changing business requirements. In the cloud, the capability to automate and test on demand lowers the risk of impact from design changes. This allows systems to evolve over time so that businesses can take advantage of innovations as a standard practice.

• **Drive architectures using data**: In the cloud you can collect data on how your architectural choices affect the behavior of your workload. This lets you make fact-based decisions on how to improve your workload. Your cloud infrastructure is code, so you can use that data to inform your architecture choices and improvements over time.

• **Improve through game days**: Test how your architecture and processes perform by regularly scheduling game days to simulate events in production. This will help you understand where improvements can be made and can help develop organizational experience in dealing with events.

The Five Pillars of the Well-Architected Framework Creating a software system is a lot like constructing a building. If the foundation is not solid structural problems can undermine the integrity and function of the building. When architecting technology solutions, if you neglect the five pillars of operational excellence, security, reliability, performance efficiency, and cost optimization it can become challenging to build a system that delivers on your expectations and requirements. Incorporating these pillars into your architecture will help you produce stable and efficient systems. This will allow you to focus on the other aspects of design, such as functional requirements. The **operational excellence** pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures. The operational excellence pillar provides an overview of design principles, best practices, and questions.

Design Principles:

There are six design principles for operational excellence in the cloud:

• **Perform operations as code**: In the cloud, you can apply the same engineering discipline that you use for application code to your entire environment. You can define your entire workload (applications, infrastructure, etc.) as code and update it with code. You can script your operations procedures and automate their execution by triggering them in response to events. By performing operations as code, you limit human error and enable consistent responses to events.

• **Annotate documentation**: In an on-premises environment, documentation is created by hand, used by people, and hard to keep in sync with the pace of change. In the cloud, you can automate the creation of documentation after every build (or automatically annotate hand-crafted documentation). Annotated documentation can be used by people and systems. Use annotations as an input to your operations code.

• **Make frequent, small, reversible changes**: Design workloads to allow components to be updated regularly. Make changes in small increments that can be reversed if they fail (without affecting customers when possible).

• **Refine operations procedures frequently**: As you use operations procedures, look for opportunities to improve them. As you evolve your workload, evolve your procedures appropriately. Set up regular game days to review and validate that all procedures are effective and that teams are familiar with them.

• **Anticipate failure**: Perform "pre-mortem" exercises to identify potential sources of failure so that they can be removed or mitigated. Test your failure scenarios and validate your understanding of their impact. Test your response procedures to ensure that they are effective and that teams are familiar with their execution. Set up regular game days to test workloads and team responses to simulated events.

• **Learn from all operational failures**: Drive improvement through lessons learned from all operational events and

DOI : 10.35291/2454-9150.2020.0073

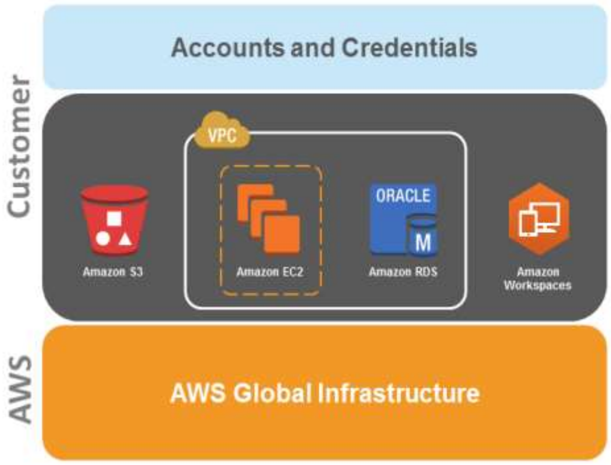
failures. Share what is learned across teams and through the entire organization.

Key AWS Services: The operational excellence-based AWS module is AWS CloudFormation, which you can use to build models based on best practices. This helps you to provide services through the production environments in an organized and consistent fashion from your creation. The following facilities and functionality support the three operational excellence areas:

- **Prepare**: AWS Config and AWS Config rules can be used to create standards for workloads and to determine if environments are compliant with those standards before being put into production.

- **Operate**: Amazon CloudWatch allows you to monitor the operational health of a workload.

- **Evolve**: Amazon Elastic search Service (Amazon ES) allows you to analyze your log data to gain actionable insights quickly and securely.



Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, providing the tools that enable customers to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of our customers' systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence. Specifically, AWS physical and operational security processes are described for the network and server infrastructure under AWS's management, as well as service-specific security implementations.

The IT infrastructure that AWS provides to its customers isdesigned and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

Power

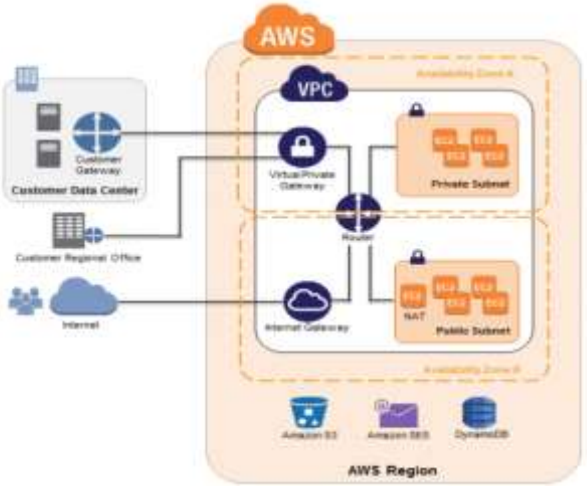
The electrical power systems at the data center are planned to be completely redundant and maintainable without effect on operations, 24 hours a day and seven days a week. Uninterruptible Power Supply (UPS) systems provide backup power for vital and necessary loads at the plant in the event of an electrical failure. Data centers use generators to provide backup power for the facility as a whole.

Climate and Temperature

To maintain a constant operating temperature for servers and other equipment, climate control is necessary, which prevents overheating and reduces the possibility of service outages. The data centers are designed to maintain optimum atmospheric conditions. Staff and equipment regulate and control temperature and humidity to appropriate levels.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that isdesigned to prevent customer data from being exposed to unauthorized individuals. All decommissioned magnetic storage devices aredegaussed and physically destroyed in accordance with industry-standard practices.



DOI : 10.35291/2454-9150.2020.0073

Amazon Glacier Security

Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where Amazon S3 is designed for rapid retrieval, Amazon Glacier is meant to be used asan archival service for data that is not accessed often and for which retrieval times of several hours are suitable.

Data Upload

You can upload an archive in a single upload operation or a multipart operation to transfer data into Amazon Glacier vaults. You can access archives up to 4 GB in size in one single upload process. Nonetheless, with the Multipart Upload API, customers can achieve better results when uploading archives greater than 100 MB. You can access large archives up to around 40 TB using the Multipart Access API. The Multipart Upload API call is designed to improve the upload experience for larger archives; it allows the pieces to be uploaded in any order and in parallel, independently.

Data Retrieval

Retrieving Amazon Glacier archives involves starting a retrieval task, which is usually completed within 3 to 5 hours. You can then access the data through requests for HTTP GET. The data will remain available to you for 24 hours. You can download a full archive from an archive, or several files.

Data Storage

Using AES-256, Amazon Glacier automatically encrypts the data and stores it in an immutable form to last. Amazon Glacier is designed to provide an archive with an average annual longevity of 99.99999999999 per cent. This stores each archive in several installations and multiple devices. Unlike traditional systems that may require laborious data verification and manual repair, Amazon Glacier conducts routine, automated data integrity checks and is designed to be self-healing automatically.

AWS Storage Gateway Security

The AWS Storage Gateway service links your on-site applications to cloud-based storage to ensure smooth and safe connectivity between your IT system and the storage infrastructure of AWS. The service allows you to securely upload data for cost-effective backup and rapid disaster recovery to AWS ' scalable, efficient, and secure Amazon S3 storage service.

AWS Storage Gateway offers three options:

• **Gateway-Stored Volumes** (where the cloud is backup). In this option, your volume data isstored locally and then pushed to Amazon S3, where it is stored in redundant, encryptedform, and made available in the form of Elastic Block Storage (EBS) snapshots. Whenyou use this model, the on-premises storage is primary, delivering low-latency access to your entire dataset, and the cloud storage is the backup.

• **Gateway-Cached Volumes** (where the cloud is primary). In this option, your volume data is stored encrypted in Amazon S3, visible within your enterprise's network via an iSCSIinterface. Recently accessed data is cached on-premises for low-latency local access.

When you use this model, the cloud storage is primary, but you get low- latency access toyour active working set in the cached volumes on premises.

• **Gateway-Virtual Tape Library** (VTL). In this option, you can configure a Gateway-VTLwith up to 10 virtual tape drives per gateway, 1 media changer and up to 1500 virtualtape cartridges. Each virtual tape drive responds to the SCSI command set, so your existing on-premises backup applications (either disk-to-tape or disk-to-disk-to-tape)will work without modification.

No matter which option you choose, data is asynchronously transferred from your on-premises storage hardware to AWS over SSL. The data is stored encrypted in Amazon S3 using Advanced Encryption Standard (AES) 256, a symmetric- key encryption standard using 256-bit encryption keys. The AWS Storage Gateway only uploads data that has changed, minimizing the amount ofdata sent over the Internet.

The AWS Storage Gateway runs as a virtual machine (VM) that you deploy on a host in your datacenter running VMware ESXi Hypervisor v 4.1 or v 5 or Microsoft Hyper-V (you download theVMware software during the setup process). You can also run within EC2 using a gateway AMI. During the installation and configuration process, you can create up to 12 stored volumes,20Cached volumes, or 1500 virtual tape cartridges per gateway. Once installed, each gateway willautomatically download, install, and deploy updates and patches.

II. Conclusion

The AWS Well-Architected Framework helps you to evaluate and develop your cloud-based systems and better understand the impact of your design decisions on the enterprise. In five conceptual areas, we discuss general design principles as well as specific best practices and guidelines which we identify as the pillars of the Well-Architected Framework.

References

[1] "Amazon Web Services: Overview of Security Processes", *White Papers*, June 2014.

[2] [online] Available: http://aws.amazon.com/what-is-aws/.

[3] Andrei Dobrin, GrigoreStamatescu, Cristian Dragana, Valentin Sgarciu, "Cloud challenges for networked

DOI : 10.35291/2454-9150.2020.0073

embedded systems: A review", *System Theory Control and Computing (ICSTCC) 2016 20th International Conference on*, pp. 866-871, 2016.

[4] BehlAkhil, BehlKanika, *An analysis of Cloud Computing Security Issues. 2012 IEEE*.

[5] Chen Deyan, Zhao Hong, *Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering*, 2012.

[6] Mladen A. Vouk, "Cloud Computing- Issues Research and Implementations", *Journal of Computing and Information Technology -CIT 16*, vol. 4, pp. 235-246, 2008.

[7] Nilesh R. Patil, Rajesh Dharmik, "Secured cloud architecture for cloud service provider", *Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) World Conference on*, pp. 1-4, 2016

[8] PrasadPadhy Rabi, Patra ManasRanjan, ChandraSatyapathy Suresh, "Cloud Computing: Security Issues and Research Challenges", *IJCSITS*, vol. 1, no. 2, December 2011.

[9] Robinson Glen, Narin Attila, Elleman Chris, "Amazon Web Services- Using AWS for Disaster Recovery", *White Papers*, October 2014.

[10] Shukla Shipra, Kumar Singh Rakesh, Security of Cloud Computing System using Object Oriented Technique, IEEE, July 2012.

[11] Zachariah PabiGariba, John Andrew Van Der Poll, "Security Failure Trends of Cloud Computing", *Collaboration and Internet Computing (CIC) 2017 IEEE 3rd International Conference on*, pp. 247-256, 2017.

[12] Zhang Qi, Cheng Lu, BoutabaRaouf, "Cloud Computing: State-of-the-art and research challenges", *J Internet ServAppl*, 2010.

DOI : 10.35291/2454-9150.2020.0073