International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 17-26

A Comprehensive Study on Amazon AWS Cloud Services and Architectural Framework

A.C.Ashmita[1], Dr.K.Santhi[2],
[1]*Research Scholar,* [2]*Associate Professor*
Department of Computer Science ,Sri Ramakrishna College of Arts & Science for Women, Coimbatore – 44, Tamilnadu, India

***Abstract*:** *As cloud computing is gaining popularity in virtualizing the data centers and increasing flexibility in the use of computing resources. This paper describes the AMAZON WEB SERVICES (AWS) cloud services and architectural framework, which helps the user to improve their knowledge on cloud-based architecture. This paper also helps in better understanding of the design principles, best practices and guidance in five areas of conceptual fields which are mentioned as pillars of amazon web services architectural framework.*
***Keywords*:** *amazon web services, architectural framework, AWS, cloud service.*

I. Introduction

AMAZON WEB SERVICES is a popular public cloud service platform which is currently used by customers across 190 countries. Amazon web service architectural framework helps to understand the pros and cons of the decision making while building systems on amazon web services. A good architectural framework system increases the likelihood of business success. This paper explains the amazon web service best practices and strategies to use when designing and operating cloud architecture.

II. Five Pillars Of Amazon Web Services Architectural Framework

The Amazon web services architectural framework is based on five pillars – security, reliability, performance efficiency, cost optimization, and operational excellence [1].

Pillar Name	Description
Security	The ability to protect information, systems, and assets while delivering business value using risk assessments and mitigation strategies.
Reliability	The ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.
Performance Efficiency	The ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.
Cost Optimization	The ability to avoid or eliminate unneeded cost or suboptimal resources.
Operational Excellence	The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

Table 1. FIVE PILLARS

A. Security

The Security pillar includes the ability to protect information, systems, and assets while delivering business value using risk assessment and mitigation strategies.

1) Design principles

In the cloud, there are a number of principles that can help to strengthen the system security.

a) *Apply security at all layers*:Rather than running security appliances (e.g., firewalls) only at the edge of the infrastructure, use firewalls and other security controls on all of the resources (e.g., every virtual server, load balancer, and network subnet) [2].
b) *Enable traceability*: Every actions and changes to the environment are logged and audited.
c) *Implement a principle of least privilege*:Ensure that authorization is appropriate for each interaction with the Amazon web service resources and implement directly strong logical access controls.
d) *Focus on securing system*:With the Amazon web service Shared Responsibility Model one can focus on securing the application, data, and operating systems, while Amazon web service provides secure infrastructure and services.
e) *Automate security best practices*:Software-based security mechanisms improve the ability to securely scale more rapidly and cost-effectively. Create and save a patched, hardened image of a virtual server, and then

use that image automatically on each new server launch. Create an entire trust zone architecture that is defined and managed in a template via revision control. Both routine and anomalous security event's response need to be automated.

2) Best Practices

There are five best practice areas for Security in the cloud:

a) ***Identity and access management*****:** The amazon web service Identity and Access Management (IAM) service, allows customers to control access to amazon web service services and resources for users which supports primarily the privilege management in amazon web service. User can apply granular policies, which assign permissions to a user, group, role, or resource. User also has the ability to require strong password practices, such as complexity level, avoiding re-use, and using multi-factor authentication (MFA). One can use federation with theexisting directory service. For workloads that require systems to have access to amazon web service, Identity and Access Management enables secure access through instance profiles, identity federation, and temporary credentials.

b) ***Detective controls*****:** One can use detective controls to identify a potential security incident. In amazon web service one can implement detective controls by processing logs, events and monitoring that allows for auditing, automated analysis, and alarming. Amazon web serviceCloudTrail logs, Amazon web service API calls, and Amazon CloudWatch provide monitoring ofmetrics with alarming, and Amazon web service Configuration providesconfiguration history. Servicelevel logs are also available, for example one can use Amazon Simple StorageService (S3) to log access requests. Finally Amazon Glacier provides a vault lockfeature to preserve mission-critical data with compliance controls designed tosupport auditable long-term retention.

c) ***Infrastructure protection*****:** Infrastructure protection includes control methodologies, such as defense in depth and multi-factor authentication, which are necessary to meet best practices and industry or regulatory obligations. In Amazon web service, one can implement stateful and stateless packet inspection, either by using Amazon web service native technologies or by using partner products and services available through the Amazon web service Marketplace. One can also use Amazon Virtual Private Cloud (VPC), to create a private, secured, and scalable environment in which one can define topology—including gateways, routing tables, and public and/or private subnets.

d) ***Data protection*****:** Before architecting any system, foundational practices that influence security should be in place. In Amazon web service, the following practices facilitate protection of data[3]:

- Amazon web service customers maintain full control over their data.
- Amazon web service makes it easier for you to encrypt your data and manage keys including regular key rotation, which can be easily automated natively by Amazon web service or maintained by a customer.
- The important content, such as file access and changes contained in detailed logging is available.
- Amazon web service has designed storage systems for exceptional resiliency. As an example, Amazon Simple Storage Service (S3) is designed for 11 nines of durability. (For example, if you store 10,000 objects with Amazon S3, one can on average expect to incur a loss of a single object once every 10,000,000 years.)
- Versioning, which can be part of a larger data lifecycle management process, can protect against accidental overwrites, deletes, and similar harm.
- Amazon web service never initiates the movement of data between regions. Content placed in a region would remain in that region unless the customer explicitly enable a feature or leverages a service that provides that functionality.

e) ***Incident response:*** Even with extremely mature preventive and detective controls, organizations should still put processes in place to respond to and mitigate the potential impact of security incidents. Putting in place the tools and access ahead of a security incident, then routinely practicing incident response will make sure the architecture is updated toaccommodate timely investigation and recovery. InAmazon web service, the following practices facilitate effective incident response:

- Detailed logging is available that contains important content, such as file access and changes.
- Events can be automatically processed and trigger scripts that automate run books through the use of Amazon web service APIs.

- One can pre-provision tooling and a "clean room" using Amazon web service Cloud Formation. This allowsto carry out forensics in a safe, isolated environment.

B. Reliability

The Reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

1) Design principles

In the cloud, there are a number of principles that can help to increase reliability.

a) ***Test recovery procedures*****:** In an on-premises environment, testing is often conducted to prove the system works in a particular scenario; testing is not typically used to validate recovery strategies. In the cloud, user can test how the system fails, and user can validate the recover procedures. User can use automation to simulate different failures or torecreate scenarios that led to failures before. This exposes failurepathways that user can test and rectify before areal failure scenario,reducing the risk of components failing that have not been tested before [4].

b) ***Automatically recover from failure*****:**By monitoring a system for key performance indicators (KPIs), user can trigger automation when athreshold is breached. This allows for automatic notification and trackingof failures, and for automated recovery processes that work around orrepair the failure. It is possible toanticipate and remediate failures before they occur with more sophisticated automation.

c) ***Scale horizontally to increase aggregate system availability:*** Replace one large resource with multiple small resources to reduce the impact of a single failure on the overall system. Distribute requests acrossmultiple, smaller resources to ensure that they do not share a commonpoint of failure.

d) ***Stop guessing capacity:***A common cause of failure in on-premisessystems is resource saturation, when the demands placed on a systemexceed the capacity of that system (this is often the objective of denial ofservice attacks). In the cloud, you can monitor demand and systemutilization, and automate the addition or removal of resources tomaintain the optimal level to satisfy demand without over- or under-provisioning.

e) ***Manage change in automation*****:**using automation the changes to the infrastructureshould be done. The changes that need to be managedare changes to the automation.

2) Best Practices

There are three best practice areas for Reliability in the cloud [5].

a) ***Foundation*****:** Before architecting any system, foundational requirements that influence reliability should be in place. For example, one must have sufficient network bandwidth to your data center. With Amazon web service, most of these foundational requirements are already incorporated or may be addressed as needed. The cloud is designed to be essentially limitless, so it is the responsibility of Amazon web service to satisfy the requirement for sufficient networking and compute capacity, while one is free to change resource size and allocation, such as the size of storage devices, on demand.

b) ***Change management*****:** Being aware of how change affects a system allows one to plan proactively, and monitoring allows one to quickly identify trends that could lead to capacity issues or SLA breaches. Using Amazon web service, one can monitor the behavior of a system and automate the response to KPIs, for example, adding additional servers as a system gains more users. One can control who has permission to make system changes and audit the history of these changes.

c) ***Failure management*****:** In any system of reasonable complexity it is expected that failures will occur, and it is generally of interest to know how to become aware of these failures, respond to them, and prevent them from happening again. One can take advantage of automation to react to monitoring data in Amazon web service,. For example, when a particular metric crosses a threshold, one can trigger an automated action to remedy the problem. Also, rather than trying to diagnose and fix a failed resource that is part of the production environment, one can replace it with a new one and carry out the analysis on the failed resource out of band. Since the cloud enables one to stand up temporary versions of a whole system at low cost, one can use automated testing to verify full recovery processes.

C. Performance Efficiency

The Performance Efficiency pillar focuses on the efficient use of computing resources to meet requirements and maintaining that efficiency as demand changes and technologies evolve.

1) Design principles

In the cloud, there are a number of principles that can help to achieve performance efficiency [6].

a) ***Democratize advanced technologies*****:** Technologies that are difficult to implement can become easier to consume by pushing that knowledge and complexity into the cloud vendor's domain. Rather than having the IT team learns how to host and run a new technology, team can simply consume it as a service. In the cloud, these technologies become services that the team can consume while focusing on product development rather than resource provisioning and management.

b) ***Go global in minutes*****:** One can easily deploy the system in multiple regions around the worldwith just a few clicks. This allows user to provide lower latency and a better experience for the customers at minimal cost.

c) ***Use serverless architectures*****:** In the cloud, server-less architectures remove the need for user to run and maintain servers to carry out traditional compute activities. For example, storage services can act as static websites, removing the need for web servers; and event services can host your code for you. This not only removes the operational burden of managing these servers, but also can lower transactional costs because these managed services operate at cloud scale.

d) **Experiment more often:** User can quickly carry out comparative testing using different types of instances, storage, or configurations with virtual and automatable resources.

e) **Mechanical sympathy:** Use the technology approach that aligns best to what users are trying to achieve. For example consider data access patterns when selecting database or storage approaches.

2) Best Practices

There are four best practice areas for Performance Efficiency in the cloud.

a) ***Selection (compute, storage, database, and network):*** The optimal solution for a particular system will vary based on the kind of workload one have, often with multiple approaches combined. Well-architected systems use multiple solutions and enable different features to improve performance. In amazon web service, resources are virtualized and are available in a number of different types and configurations. This makes it easier to find an approach that closely matches with needs, and can also find options that are not easily achievable with on-premises infrastructure. For example, a managed service such as Amazon DynamoDB provides a fully managed NoSQL database with single-digit millisecond latency at any scale.

b) ***Review*****:** When architecting solutions, there is a finite set of options that one can choosefrom. However, over time new technologies and approaches become availablethat could improve the performance of the architecture.Using Amazon web service, one can take advantage of our continual innovation, which is drivenby customer need. We release new regions, edge location, services, and featuresregularly. Any of these could positively improve the performance efficiency of the architecture.

c) ***Monitoring:*** Once one has implemented the architecture one will need to monitor its performance so that you can remediate any issues before your customers are aware. Monitoring metrics should be used to raise alarms when thresholds are breached. The alarm can trigger automated action to work around any badly performing components. Using amazon web service, Amazon CloudWatch provides the ability to monitor and send notification alarms, and one can use automation to work around performance issues by triggering actions through Amazon Kinesis, Amazon Simple Queue Service (SQS), and AWS Lambda [4].

d) ***Tradeoffs*****:** When need to architect solutions, think about trade-offs so one can select an optimal approach. Depending on the situation that could trade consistency, durability, and space versus time or latency, to deliver higher performance. Using amazon web service can go global in minutes and deploy resources in multiple locations across the globe to becloser to end users. One can also dynamically add read-only replicas to information stores such as database systems to reduce the load on the primary database. AWS also offers caching solutions such as Amazon ElastiCache, which provides an in-memory data store or cache, and Amazon CloudFront, which caches copies of the static content closer to end-users.

D. Cost Optimization

The Cost Optimization pillar includes the continual process of refinement and improvement of a system over its entire lifecycle. From the initial design of your very first proof of concept to the ongoing operation of production workloads, adopting the practices in this paper will enable user to build and operate cost-aware systems that achieve business outcomes and minimize costs, thus allowing the business to maximize its return on investment [7].

1) Design principles

In the cloud user can follow a number of principles that help to achieve cost optimization.

a) ***Adopt a consumption model*****:** Pay only for the computing resources that user consume and increase or decrease usage depending on business requirements, not by using elaborate forecasting. For example, *development and test environments are typically only used for eight hours a day during the work week. One* can stop these resources when they are not in use for a potential cost savings of 75 percent (40 hours versus 168 hours).

b) ***Benefit from economies of scale*****:** By using cloud computing, user may achieve a lower variable cost than could on own because Amazon web service can achieve higher economies of scale. Hundreds of thousands of customers are aggregated in the Amazon web service Cloud, which translates into lower pay-as-you-go prices.

c) ***Stop spending money on data center operations*****:** Amazon web service does the heavy lifting of racking, stacking, and powering servers, so user can focus on the customers and business projects rather than on IT infrastructure.

d) ***Analyze and attribute expenditure*****:** The cloud makes it easier to accurately identify the usage and cost of systems, which then allowstransparent attribution of IT costs to individual business owners. Thishelps measure return on investment (ROI) and gives system owners an opportunity to optimize their resources and reduce costs.

e) ***Use managed services to reduce cost of ownership*****:** The operational burden of maintaining servers for tasks like sending email or managing databases are removed by cloud, managed services. And because managed services operate at cloud scale, they can offer a lower cost per transaction or service.

2) Best Practices

There are four best practice areas for Cost Optimization in the cloud.

a) ***Cost-effective resources*****:** Using the appropriate instances and resources for the system is keyto cost savings. A well-architected system will use the most cost-effective resources, which can have a significant and positive economic impact. One also has the opportunityto use managed services to reduce costs. For example, rather than maintaining servers to deliver email, can use a service that charges on a per-message basis. Amazon web service offers a variety of flexible and cost-effective pricing options to acquire Amazon EC2 instances in a way that best fits the needs. On-Demand Instances allow one to pay for compute capacity by the hour, with no minimum commitments required. Reserved Instances (RIs) allow one to reserve capacity and offer savings of up to 75 percent off On-Demand pricing. With Spot Instances, one can bid on unused Amazon EC2 capacity at significant discounts. Spot Instances are appropriate where the system can tolerate using a fleet ofservers where individual servers can come and go dynamically, such as when using HPC and big data.

b) ***Matching supply and demand:*** Optimally matching supply to demand delivers the lowest costs for a system, butthere also needs to be sufficient extra supply to allow for provisioning time and individual resource failures. Demand can be fixed or variable, requiring metricsand automation to ensure that management does not become a significant cost. In amazon web service, one can automatically provision resources to match demand. Auto Scaling and demand, buffer, and time based approaches allow to add and remove resources as needed. If one can anticipate changes in demand, one can save more money and ensure the resources match the system needs.

c) ***Expenditure awareness*****:** The increased flexibility and agility that the cloud enables encourages innovation and fast-paced development and deployment. It eliminates the manual processes and time associated with provisioning on-premises infrastructure, including identifying hardware specifications, negotiating price quotations, managing purchase orders, scheduling shipments, and then deploying the resources. However, the ease of use and virtually unlimited on-demand capacity may require a new way of thinking about expenditures. Many businesses are composed of multiple systems run by various teams. The capability to attribute resource costs to the individual business or product owners drives efficient usage behavior and helps reduce waste. Accurate cost attribution also allows one to understand which products are truly profitable, and allows making more informed decisions about where to allocate budget.

d) ***Optimizing over time*****:** It is a best practice to review existing architectural decisions to ensure they continue to be the most cost-effective, as Amazon web service releases new services and features.As the requirements change, be aggressive in decommissioningresources and entire services, or systems that you no longer require. Managed services from Amazon web service can often significantly optimize a solution, so it is good to be aware of new managed services as they become available. Forexample, running an Amazon RDS database can be cheaper than running own database on Amazon EC2.

III. Operational Excellence

The Operational Excellence pillar includes operational practices and procedures used to manage production workloads. This includes how planned changes are executed, as well as responses to unexpected operational events.Change execution and responses should be automated. All processes and procedures of operational excellence should be documented, tested, and regularly reviewed [8].

1) Design principles

In the cloud, there are a number of principles that drive operational excellence.

a) ***Perform operations with code*****:** Use automation, when there are common repetitive processes or procedures. For example, consider automating configuration management, changes, and responses to events.

b) ***Align operations processes to business objectives*****:** Collect metrics that indicate operational excellence in meeting business objectives. The goal should be to reduce the signal to noise ratio in metrics, so operational monitoring and responses are targeted to support business-critical needs. Collecting metrics that are unnecessary will prevent effective responses to unexpected operational events by complicating monitoring and response.

c) ***Make regular, small, incremental changes*****:** Workloads should be designed to allow components to be updated regularly. Changes should be done in small increments, not large batches, and should be able to berolled back without affecting operations. Put operations procedures in place to allow for the implementation of those changes without downtime for maintenance or the replacement of dependent service components.

d) ***Test for responses to unexpected events*****:** Workloads should be tested for component failures and other unexpected operational events. It is important to test and understand procedures for responding to operational events, so that they are followed when operational events occur. To test responses to simulated operational events and failure injections set up game days.

e) ***Learn from operational events and failures*****:** Processes should be in place so that all types of operational events and failures are captured, reviewed, and then used for improvements. Regular cross-functional operations reviews should result in process improvements that driveoperational excellence.

f) ***Keep operations procedures current*****:** Process and procedure guides should be adapted as environments and operations evolve. This includes updating regular operations runbooks (standard operations procedures), as well as playbooks (response plans for unexpected operational events or production failures). Guidance and learning for operations should be shared between teams to prevent repeated mistakes. Consider using a wiki or an internal knowledge base for this information. The information that should be evaluated includes operations metrics, unexpected anomalies, failed deployments, system failures, and ineffective or inappropriate responses to failures. System and architecture documentation should also be captured and updated using automation as environments and operations evolve.

2) Best Practices

There are three best practice areas for Operational Excellence in the cloud [9].

a) ***Preparation*****:** To drive operational excellence, preparation is essential Operational readiness include manual cross functional or peer reviews to ensure oversight. Amazon web service services such as Amazon web service CloudFormation can be used to ensure that environments contain all required resources when deployed in production, and that theconfiguration of the environment is based on tested best practices, which reduces the opportunity for human error. Implementing Auto Scaling, or other automated scaling mechanisms, will allow workloads to automatically respondwhen business-related events affect operational needs. Services like Amazon web service Config with the Amazon web service Config rules feature create mechanisms to automatically track and respond to changes in Amazon web service workloads and environments. It is also important to use features like tagging to make sure all resources in a workload can be easily identified when needed during operations and responses.

b) ***Operations:*** Operations process and procedures must be thoroughly planned, tested, reviewed. Workloads should evolve and be changed in automated and manageable ways. Changes should be small, frequent, and incremental, all without impacting continuous operations. In Amazon web service one can set up a continuous integration / continuous deployment (CI/CD) pipeline (e.g., source code repository, build systems, deployment and testing automation). Release management processes, whether manual or automated, should be tested and be based on small incremental changes, and tracked versions. One should be able to revert changes that introduce operational issues without causing operational impact. Change quality assurance should include risk mitigation strategies such as Blue/Green, Canary, and A/B testing. Operations checklists should be used to evaluate a workload'sreadiness for production. Aggregate logs for

centralized monitoring and alerts. Make sure alerts trigger automated responses, including notification and escalations. Also design monitors for anomalies, not just failures.

c) ***Responses*****:** Operations teams must be prepared to respond to operational events and failures, and have processes in place tolearn from them. In Amazon web service there are several mechanisms to ensure both appropriate alerting andnotification in response to unplanned operational events, as well as automated responses. Based on all available logs and metrics, tools should also be in place to centrally monitor workloads and create effective alerts and notifications.

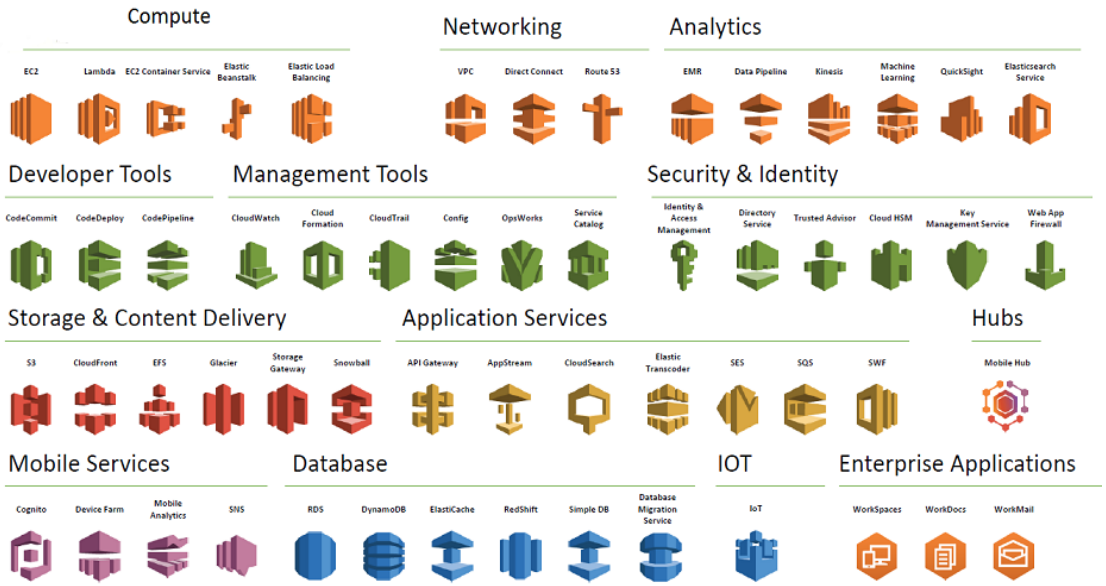

Fig.1. Tools of AWS

IV. Key Amazon Web Service Services

E. Security

The Amazon web service that is essential to security is amazon web service. Identity and AccessManagement (IAM), which allows you to securely control access to Amazon web services services and resources for users. The following services and featuressupport the four areas of security.

1) Identity and access management

Identity and AccessManagement (IAM) enables to securely control access to AWS services and resources. Multi-factor authentication (MFA), adds an extra layer of protection on top of the user name and password.

2) Detective controls

Amazon web service CloudTrail records Amazon web service API calls, Amazon web service Config provides detailed inventory of the Amazon web service resources and configuration, and Amazon CloudWatch is a monitoring service for AWS resources.

3) Infrastructure protection

Amazon Virtual Private Cloud (VPC) lets one provision a private, isolated section of the AWS Cloud where one can launch AWS resources in a virtual network[10].

4) Data protection

Services such as Elastic Load Balancing, Amazon Elastic Block Store (EBS), Amazon Simple Storage Service (S3), and Amazon Relational Database Service (RDS) include encryption capabilities to protect the data intransit and at rest. For customers to easily create and control keys, AWS Key Management Service (KMS) is used for encryption.

5) Incident response

Identity and AccessManagement (IAM) should be used to grant appropriate authorization to incident response teams. A trusted environment for conducting investigations can be created by Amazon CloudFormation.

F. Reliability

The AWS service that is a key to ensuring reliability is Amazon CloudWatch, which monitors run-time metrics. Other services and features that support the three areas of reliability are as follows.

1) Foundations

Amazon web service Identity and Access Management (IAM) enables you to securely control access to AWS services and resources. Amazon VPC lets one provision a private, isolated section of the AWS Cloud where one can launchAmazon web service resources in a virtual network.

2) Change management

Amazon web service CloudTrail records AWS API calls for the account and delivers log files to you for auditing. Amazon web service Config provides a detailed inventory of your Amazon web service resources and configuration, and continuously records configuration changes.

3) Failure management

AWS CloudFormation provides templates for the creation of AWS resources and provisions them in an orderly and predictable fashion.

G. Performance efficiency

The key Amazon web service service for performance efficiency is Amazon CloudWatch, which monitors the resources and systems, providing visibility into overallperformance and operational health. The following services are important in the areas of performance efficiency [11].

1) Selection

a) Compute

Auto Scaling is key to ensuring that one have enough instances to meet demand and maintain responsiveness.

b) Storage

Amazon EBS provides a wide range of storage options (such as SSD and provisioned input/outputoperations per second (PIOPS)) that allow you to optimize for use case. Amazon S3 provides serverless content delivery and Amazon S3 Transfer Acceleration enables fast, easy and secure transfers of files over long distances.

c) Database

Amazon RDS provides a wide range of database features (such as provisioned IOPS and read replicas) that allow to optimize for use case. Single-digit millisecond latency atany scale is provided by AmazonDynamoDB.

d) Network

Amazon Route 53 provides latency-based routing. Amazon VPC endpoints and Direct Connect can reducenetwork distance or jitter [12].

2) Review

The AWS Blog and what isnew section on the AWS website are resources for learning about newly launched features and services.

3) Monitoring

Amazon CloudWatch provides metrics, alarms, and notifications that you can integrate with your existing monitoring solution, and that one can use with AWS Lambda to trigger actions.

4) Tradeoff

Amazon ElastiCache, Amazon CloudFront, and AWS Snowball are services that allow to improve performance. Read replicas in Amazon RDS can allow to scale read-heavy workloads.

H. Cost Optimization

The key Amazon web service feature that supports cost optimization is cost allocation tags, which help one to understand the costs of a system. The following services andfeatures are important in the four areas of cost optimization [13].

1) Cost-effective resources

One can use Reserved Instances and prepaid capacity to reduce the cost. Amazon web service Trusted Advisor can be used to inspect the Amazon web service environment and find opportunities to save money.

2) Matching supply and demand
One can add or remove resources to match demand without overspending sing Auto Scaling.

3) Expenditure awareness
Amazon CloudWatch alarms and Amazon Simple Notification Service (SNS) notifications will warn if onego over, or are forecasted to go over, the budgeted amount.

4) Optimizing over time
The Amazon web service Blog and the What's New section on the Amazon web service website are resources for learning about newly launched features and services. Amazon web service Trusted Advisor inspects the Amazon web service environment and finds opportunities to save money by eliminating unused or idle resources or committing to Reserved Instance capacity.

E. Operational Excellence

There are two primary services that can be used to drive operational excellence. Amazon web service CloudFormation can be used to create templates based on best practices, and provision resources in an orderly and predictable fashion. Amazon CloudWatch can be used for monitoring metrics, collecting logs, generating alerts, and triggering responses. Other services and features that support the three areas of Operational Excellence are as follows [14].

1) Preparation
Amazon web service Config provides a detailed inventory of the Amazon web service resources and configuration, and continuously records configuration changes. Amazon web service (AWS) Service Catalog helps to create a standardized set of service offerings that are aligned to best practices. Designing workloads that use automation with services like Auto Scaling, and Amazon SQS, are good methods to ensure continuous operations in the event of unexpected operational events.

2) Operations
Amazon web service CodeCommit, Amazon web service CodeDeploy, and Amazon web service CodePipelinecan be used to manage and automate code changes to Amazon web service workloads. Use Amazon web service SDKs or third-party libraries to automate operational changes. To audit and track changes made to Amazon web service environments use Amazon web service CloudTrail.

3) Responses
Take advantage of all of the Amazon CloudWatch service features for effective and automated responses. Amazon CloudWatch alarms can be used to set thresholds for alerting and notification, and Amazon CloudWatch events can trigger notifications and automated responses.

Fig. 2. Amazon web service infrastructure and services

V. Conclusion

The Amazon web service Architectural Framework provides architectural best practices across five pillars for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. The framework provides a set of questions that allows to review an existing or proposed architecture, and also a set of Amazon web service best practices for each pillar. Using the framework in the architecture will help produce stable and efficient systems, which allows to focus on functional requirements.

References

[1]. George Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O'Reilly, April 2009.
[2]. Jeff Barr, "AWS Elastic Load Balancing Inside of a Virtual Private Cloud", Amazon Web Services Blog 2011.Available at http://aws.typepad.Com/aws/2011/11/new-aws-elastic-load-balancing-inside-Of-a-virtual-private- cloud.html.
[3]. "Amazon Web Services: Overview of Security Processes", White Papers, June 2014.
[4]. Glen Robinson, Attila Narin, and Chris Elleman."Amazon Web Services- Using AWS for Disaster Recovery", White Papers, October 2014.
[5]. Athman Bouguettaya, Quan Z. Sheng and Florian Daniel," Advanced Web Services", Springer, 2014.
[6]. Amit Shah, Aurobindo Sarkar, Learning AWS, packt publishing, 2015.
[7]. Kevin Miller, Steve Morad, Minoo Duraipandy," Overlay Multicast in Amazon Virtual Private Cloud", Article, April 29, 2015.
[8]. Mr.Arabolu Chandra Sekhar, Dr. R. Praveen Sam, A WALK THROUGH OF AWS (AMAZON WEB SERVICES), *International Research Journal of Engineering and Technology (IRJET)*, Volume: 02 Issue: 03 | June-2015.
[9]. "An introduction to high performance computing on Aws Available", White paper, August 2015, Available at https://d0.awsstatic.com/whitepapers/Intro_to_HPC_on_AWS.pdf.
[10]. "Amazon web server networking concept", Document, 2016, Available at https://aws.amazon.com/documentation/vpc/?icmpid=docs.
[11]. "An introduction to Aws", blog location, 2016, Available at https://aws.amazon.com/blogs/aws/?nc1=f_so.
[12]. George Sammons, Introduction to amazon web services beginner's guide book: Learning the basics of AWS in easy and fast way, 2016.
[13]. Re invent on aws, Conference, venturebeat.com/2016/11/30/aws-reinvent-2016/, Nov 30, 2016.
[14]. "Overview of Amazon Web Services", White papers, April 2017, https://aws.amazon.com.